Australian Government
Australian Law Reform Commission

Review of Australian Privacy Law

DISCUSSION PAPER

You are invited to provide a submission or comment on this Discussion Paper

VOLUME 1
DISCUSSION PAPER 72
SEPTEMBER 2007

This Discussion Paper reflects the law as at 31 July 2007

ISBN- 978-0-9758213-9-8

Commission Reference: DP 72

The Australian Law Reform Commission was established on 1 January 1975 by the *Law Reform Commission Act 1973* (Cth) and reconstituted by the *Australian Law Reform Commission Act 1996* (Cth). The office of the ALRC is at Level 25, 135 King Street, Sydney, NSW, 2000, Australia.

All ALRC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the ALRC.

Telephone:	within Australia	(02)	8238 6333
	International	+61 2	8238 6333
TTY:		(02)	8238 6379
Facsimile:	within Australia	(02)	8238 6363
	International	+61 2	8238 6363

E-mail: info@alrc.gov.au

ALRC homepage: www.alrc.gov.au

Printed by Ligare Pty Ltd

Making a submission

Any public contribution to an inquiry is called a submission and these are actively sought by the ALRC from a broad cross-section of the community, as well as those with a special interest in the inquiry.

Submissions are usually written, but there is no set format and they need not be formal documents. Where possible, submissions in electronic format are preferred.

It would be helpful if comments addressed specific proposals and questions or numbered paragraphs in this paper.

Open inquiry policy

In the interests of informed public debate, the ALRC is committed to open access to information. As submissions provide important evidence to each inquiry, it is common for the ALRC to draw upon the contents of submissions and quote from them or refer to them in publications. As part of ALRC policy, non-confidential submissions are made available to any person or organisation upon request after completion of an inquiry, and also may be published on the ALRC website. For the purposes of this policy, an inquiry is considered to have been completed when the final report has been tabled in Parliament.

However, the ALRC also accepts submissions made in confidence. Confidential submissions may include personal experiences where there is a wish to retain privacy, or other sensitive information (such as commercial-in-confidence material). Any request for access to a confidential submission is determined in accordance with the federal *Freedom of Information Act 1982*, which has provisions designed to protect sensitive information given in confidence.

In the absence of a clear indication that a submission is intended to be confidential, the ALRC will treat the submission as non-confidential.

Submissions should be sent to:

The Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001
Email: privacy@alrc.gov.au

Submissions may also be made using the online form on the ALRC's homepage:

<www.alrc.gov.au>

The closing date for submissions in response to DP 72 is Friday 7 December 2007.

Contents

Terms of Reference **15**
List of Participants **17**
List of Proposals and Questions **21**
List of Proposed Unified Privacy Principles **89**

Volume 1

Part A – Introduction 101

1. Introduction to the Inquiry **103**
Introduction 103
Key proposals for reform 105
Background 107
Privacy Act 110
The scope of the Inquiry 111
Related privacy references 112
Defining 'privacy' 114
Privacy beyond the individual 122
Organisation of this paper 136
Process of reform 140

2. Overview—Privacy Regulation in Australia **145**
Introduction 145
The *Australian Constitution* and privacy 145
Federal regulation of privacy 146
State and territory regulation of privacy 148
Legislative rules, codes and guidelines 167
Non-legislative rules, codes and guidelines 168

3. The *Privacy Act* **169**
Introduction 169
Overview of the *Privacy Act* 171
The structure of the Act 182
The name of the Act 184
The objects of the Act 187
Some important definitions 194
Deceased individuals 219

4. Achieving National Consistency **235**
Introduction 235
The federal system 237
Is national consistency important? 238
National legislation 241
Commonwealth-state cooperative scheme 247
A model for national consistency 253
A permanent standing body 262
A single privacy regulator? 267
Other methods to achieve national consistency 270

5. Protection of a Right to Personal Privacy **277**
Introduction 277
Background 278
Right to personal privacy—developments in Australia and elsewhere 280
NSWLRC Consultation Paper on invasion of privacy 290
Recognising an action for breach of privacy in Australia 291
ALRC's view 294

Part B – Developing Technology **309**

6. Overview—Impact of Developing Technology on Privacy **311**
Introduction 311
Privacy enhancing technologies 312
The internet 315
Radio frequency identification 321
Other wireless technologies 325
Data-matching and data-mining 325
Smart cards 327
Biometric technologies 330
DNA-based technologies 333
Voice over internet protocol 334
Location detection technologies 335
Surveillance technologies 337
Other developing technologies 339

7. Accommodating Developing Technology in a Regulatory Framework **341**
Introduction 341
Should the *Privacy Act* be technologically neutral? 342
Designing a 'technologically aware' framework 346
Statutory protection 350
Standards 354
The role of the regulator 358

Proactive regulation 358
Oversight functions of the OPC 359
Guidance on particular technologies 361
Co-regulation 372
Other regulatory mechanisms 374

8. Individuals, the Internet and Generally Available Publications 375
Introduction 375
Individuals acting in a personal capacity 376
Generally available publications 383

9. Identity Theft 393
Introduction 393
What is identity theft? 394
How prevalent is it? 395
Criminalising identity theft 396
Other responses to identity theft 398
Identity theft and privacy laws 399

Part C – Interaction, Inconsistency and Fragmentation 404

10. Overview—Interaction, Inconsistency and Fragmentation 405
Introduction 405
The costs of inconsistency and fragmentation 406
Federal information laws 408
Required or authorised by or under law 412
Interaction with state and territory laws 415

11. The Costs of Inconsistency and Fragmentation 419
Introduction 419
Sharing information 420
Compliance burden and cost 428
Multiple regulators 435
Government contractors 438

12. Federal Information Laws 447
Introduction 447
Terms and definitions 447
Freedom of Information Act 1982 (Cth) 449
Archives Act 1983 (Cth) 468

A single information Act? 472
A single regulator? 474
Secrecy provisions 476
Obligations of confidence 482

13. Required or Authorised by or Under Law 487
Introduction 487
'Required or authorised by or under law' 487
Census and Statistics Act 1905 (Cth) 498
Corporations Act 2001 (Cth) 502
Commonwealth Electoral Act 1918 (Cth) 506
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) 510

14. Interaction with State and Territory Laws 519
Introduction 519
Interaction of federal, state and territory regimes 519
Privacy rules, codes and guidelines 526
Residential tenancy databases 528

Volume 2

Part D – The Privacy Principles 541

15. Structural Reform of the Privacy Principles 543
Introduction to Part D 543
Development of current Australian privacy principles 544
Principles-based regulation of privacy 548
Level of detail, guidance and protection 554
Towards a single set of privacy principles 560
Scope and structure of Unified Privacy Principles 567

16. Consent 571
Introduction 571
'Consent' and 'bundled consent' in the *Privacy Act* 572
A separate privacy principle dealing with consent? 583

17. Anonymity and Pseudonomity 587
Introduction 587
Expansion of anonymity principle 588
The option to transact anonymously or pseudonymously 593
Summary of proposed 'Anonymity and Pseudonymity' principle 597

18. Collection **599**
Introduction 599
Collection from the individual 601
Unsolicited personal information 605
Other aspects of the 'Collection' principle 608
Summary of proposed 'Collection' principle 610

19. Sensitive Information **613**
Introduction 613
Expansion of sensitive information principle to agencies? 615
Regulation of other aspects of sensitive information handling 618
Emergency situations 622
Research 625

20. Specific Notification **627**
Introduction 627
Location of notification requirements: separate principle? 628
Notification of collector's identity and individual's rights 630
Notification of the fact and circumstances of collection 633
Standardising requirements of agencies and organisations 635
Notification where information collected from a third party 640
Meaning of 'reasonable steps' 645
Summary of proposed 'Specific Notification' principle 648

21. Openness **651**
Introduction 651
Separate 'Openness' principle? 652
Regulatory structure: 'Privacy Policies' 654
Matters to be included in a Privacy Policy 656
Availability of Privacy Policy 660
Short form privacy notices 662
Summary of proposed 'Openness' principle 664

22. Use and Disclosure **667**
Introduction 667
Towards a single 'Use and Disclosure' principle 670
Use and disclosure of personal information for a related secondary purpose 674
Emergencies, disasters and threats to life or health 679
Missing persons 685
Disclosure of 'incidents' by insured professionals to insurers 688
Use and disclosure in other contexts 690
Logging disclosures 694

Summary of proposed 'Use and Disclosure' principle 697

23. Direct Marketing 699
Introduction 699
Direct marketing generally 701
Scope of direct marketing privacy principle 703
Relationship between privacy principles and other legislation 706
Opt-in or opt-out requirement? 708
Other possible requirements 713
Summary of proposed 'Direct Marketing' principle 716

24. Data Quality 719
Introduction 719
Application of data quality principle to agencies 720
Scope of data quality principle 721
Clarification of data quality principle 726
Summary of proposed 'Data Quality' principle 727

25. Data Security 729
Introduction 729
Towards a single data security principle 731
Protection of personal information 733
Destruction versus retention of personal information 739
Extension of destruction and de-identification requirements to agencies 741
When is destruction or deletion appropriate? 745
General right to destruction of personal information? 748
Meaning of 'destroy or permanently de-identify' 750
Summary of proposed 'Data Security' principle 753

26. Access and Correction 755
Introduction 755
Scope of proposed 'Access and Correction' principle 757
Access by intermediaries 759
Barriers to access: fees and timeframe 761
Right to correction of personal information 763
Incorrect information: notification of third parties 765
Consequential amendments 769
Notification of access rights 770
Summary of proposed 'Access and Correction' principle 771

27. Identifiers 775
Introduction 776
Separate principle to regulate identifiers? 778

Application of 'Identifiers' principle to agencies? 779
Definition of 'identifier' 783
Content of privacy principle dealing with identifiers 787
Unique multi-purpose identifiers 794
Regulation of Tax File Numbers 805
Summary of proposed 'Identifiers' principle 811

28 Transborder Data Flows 815
Introduction 815
Extra-territorial operation of the *Privacy Act* 817
National Privacy Principle 9 821
Related bodies corporate 836
The role of the Privacy Commissioner 838
Requirement of notice that personal information is being sent overseas 844
International privacy protection 848
Summary of proposed 'Transborder Data Flows' principle 862

29. Additional Privacy Principles 865
Introduction 865
Accountability principle 866
Prevention of harm principle 869
No disadvantage principle 872

Part E – Exemptions 875

30. Overview—Exemptions from the *Privacy Act* 877
Introduction 877
Exemptions under the *Privacy Act* 878
Exemptions under international instruments 881
Should there be any exemptions from the *Privacy Act*? 883
The number and scope of exemptions 887
Complexity of the exemption provisions 892
Location of the exemption provisions 894

31. Defence and Intelligence Agencies 899
Introduction 899
The exempt agencies 900
Rationale for the exemption of the AIC agencies 903
Issues concerning the exemption of the IGIS 916
Submissions and consultations 918
ALRC's view 922

32. Federal Courts and Tribunals **927**
Introduction 927
Federal courts 927
Federal tribunals 942

33. Exempt Agencies under the *Freedom of Information Act 1982* (Cth) **955**
Introduction 955
Australian Fair Pay Commission 956
Schedule 2 Part I Division 1 of the *Freedom of Information Act* 959
Schedule 2 Part II Division 1 of the *Freedom of Information Act* 963
ALRC's view 971

34. Other Public Sector Exemptions **975**
Introduction 976
Royal commissions 976
Australian Crime Commission 978
Integrity Commissioner 987
Other agencies with law enforcement functions 991
Parliamentary departments 994
State and territory authorities and prescribed instrumentalities 996

35. Small Business Exemption **1007**
Introduction 1007
Current law 1007
Retention of the exemption 1010
Removal of the exemption 1019
Voluntary compliance and opting in 1035
ALRC's view 1036

36. Employee Records Exemption **1039**
Introduction 1039
Current law 1039
Adequacy of privacy protection for employee records 1043
Evaluative material 1056
Location of privacy provisions concerning employee records 1061

37. Political Exemption **1065**
Introduction 1065
Current law 1065
Government inquiries 1069
International instruments 1070
Electoral databases 1071
Implied freedom of political communication 1072

Submissions and consultations 1073
ALRC's view 1077

38. Media Exemption 1081
Introduction 1081
Scope of the exemption 1090
Criteria for media privacy standards 1100
Adequacy of the self-regulatory and co-regulatory models 1106
Enforcement mechanisms 1110

39. Other Private Sector Exemptions 1113
Introduction 1113
Personal or non-business use 1113
Related bodies corporate 1115
Change in partnership 1121

40. New Exemptions 1123
Introduction 1123
New exemptions and partial exemptions 1123
Declared emergencies 1137

Part F – Office of the Privacy Commissioner 1141

41. Overview—Office of the Privacy Commissioner 1143
Introduction 1143
Facilitating compliance with the *Privacy Act* 1144
Structure of the OPC 1145
Powers of the OPC 1146
Investigation and resolution of privacy complaints 1147
Enforcing the *Privacy Act* 1148
Data breach notification 1148
Summary of proposals to address systemic issues 1149

42. Facilitating compliance with the *Privacy Act* 1151
Introduction 1151
Compliance-oriented approach to privacy regulation 1152

43. Structure of the Office of the Privacy Commissioner 1159
Introduction 1160
Structure, functions and powers 1160
Manner of exercise of powers 1166

Accountability mechanisms 1169
Criminal liability 1172
Immunity 1172
Privacy Advisory Committee 1175

44. Powers of the Office of the Privacy Commissioner 1185
Introduction 1186
Oversight powers 1186
Guidelines 1193
Personal Information Digest 1196
Privacy impact assessments 1199
Compliance powers 1210
Audit functions 1211
Self-auditing 1218
Functions under other Acts 1221
Public interest determinations 1223
Privacy codes 1226

45. Investigation and Resolution of Privacy Complaints 1239
Introduction 1239
Investigating privacy complaints 1240
Transferring complaints to other bodies 1244
Resolution of privacy complaints 1248
Accountability and transparency 1259
Other issues in the complaint-handling process 1264

46. Enforcing the *Privacy Act* 1275
Introduction 1275
Enforcing own motion investigations 1276
Enforcing a determination 1279
Reports by the Commissioner 1281
Injunctions 1281
Other enforcement mechanisms following non-compliance 1283

47. Data Breach Notification 1293
Overview 1293
Rationale for data breach notification 1294
Models of data breach notification laws 1297
Submissions and consultations 1306
ALRC's view 1309

Volume 3

Part G – Credit Reporting Provisions 1321

48. Overview—Credit Reporting 1323
Introduction 1323
What is credit reporting? 1325
Credit reporting agencies 1327
Background to national regulation 1328
Legislative history 1331

49. The Credit Reporting Provisions 1337
Introduction 1337
Application of the credit reporting provisions 1339
Content of credit information files 1342
Accuracy and security of personal information 1345
Disclosure of personal information 1346
Use of personal information 1350
Rights of access, correction and notification 1352
Responsibilities and powers of the OPC 1353
Remedies and penalties 1358

50. The Approach to Reform 1359
Introduction 1359
Part IIIA and the NPPs 1360
Options for reform 1362
Repeal and new regulation under the Act 1363
Approaches to the new credit reporting regulations 1372
Application of the regulations 1377
Credit reporting industry code 1398

51. More Comprehensive Credit Reporting 1401
Introduction 1401
'Positive' or 'more comprehensive' credit reporting? 1402
Australia's approach to more comprehensive credit reporting 1404
The argument for more comprehensive credit reporting 1408
Benefits of more comprehensive credit reporting 1409
Problems with more comprehensive credit reporting 1418
Empirical studies 1421
Regulation in other jurisdictions 1426
Models of more comprehensive credit reporting 1429

Privacy safeguards 1436
Should more comprehensive reporting be permitted? 1437
ALRC's view 1440

52. Collection of Credit Reporting Information 1445
Introduction 1445
Collection and notification 1446

53. Use and Disclosure of Credit Reporting Information 1475
Introduction 1475
Use and disclosure 1475
Consent and credit reporting 1497

54. Data Quality and Security 1503
Introduction 1503
Data quality 1504
Improving data quality 1513
Regulating data quality 1520
Deletion of credit reporting information 1523
Data security 1526

55. Rights of Access, Complaint Handling and Penalties 1529
Introduction 1529
Access and correction 1529
Complaint handling 1540
Penalties 1554

Part H – Health Services and Research 1557

56. Regulatory Framework for Health Information 1559
Introduction 1559
National consistency 1561
A separate set of Health Privacy Principles? 1570
Electronic health information systems 1581

57. The *Privacy Act* and Health Information 1595
Introduction 1595
Privacy Act 1988 (Cth) 1595
Privacy (Health Information) Regulations 1614

58. Research **1653**
Introduction 1653
The current arrangements 1654
Research other than health and medical research 1663
Definition of research 1667
The public interest balance 1670
Impracticable to seek consent 1676
Human Research Ethics Committees 1681
An exception to the proposed Unified Privacy Principles 1689
Identifiable personal information 1692
Databases and data linkage 1699

Part I – Children, Young People and Adults Requiring Assistance **1713**

59. Children, Young People and Privacy **1715**
Introduction 1715
Generational difference 1716
Attitudes of young people 1719
ALRC consultations with young people 1723
Online social networking 1728
Photographs and other images 1735
ALRC's view 1744

60. Decision Making by Individuals Under the Age of 18 **1751**
Introduction 1751
Privacy rights of children and young people at international law 1753
Existing Australian laws relating to privacy of individuals under the age of 18 1756
Assessing the decision-making capacity of children and young people 1759
Specific privacy issues affecting children and young people 1787

61. Adults with a Temporary or Permanent Incapacity **1815**
Introduction 1815
Equality and the presumption of capacity 1816
Problems with the *Privacy Act* 1819
Suggestions for reform 1822
ALRC's view 1829

62. Other Third Party Assistance **1839**
Introduction 1839

Problems with the *Privacy Act* in practice 1839
Existing third party arrangements 1841
ALRC's view 1844

Part J – Telecommunications 1847

63. *Telecommunications Act* 1849
Introduction 1849
Telecommunications Act 1997 (Cth) 1851
Are two privacy regimes necessary? 1853
Does the *Telecommunications Act* provide adequate privacy protection? 1858
Interaction between the *Privacy Act* and the *Telecommunications Act* 1859
Exceptions to the use and disclosure offences 1860
Integrated public number database 1878
Small business exemption 1889
Criminal or civil penalties 1891
New technologies 1893
Telecommunications regulators 1896
A redraft of the Part 1899

64. Other Telecommunications Privacy Issues 1901
Introduction 1901
Interception and access 1901
Spam and telemarketing 1916
Telecommunications regulators 1930

Appendix 1. List of Submissions 1939
Appendix 2. List of Agencies, Organisations and Individuals Consulted 1955
Appendix 3. List of Abbreviations 1965

Terms of Reference

REVIEW OF THE PRIVACY ACT 1988

I, Philip Ruddock, Attorney-General of Australia, having regard to:

- the rapid advances in information, communication, storage, surveillance and other relevant technologies
- possible changing community perceptions of privacy and the extent to which it should be protected by legislation
- the expansion of State and Territory legislative activity in relevant areas, and
- emerging areas that may require privacy protection,

refer to the Australian Law Reform Commission for inquiry and report pursuant to subsection 20(1) of the *Australian Law Reform Commission Act 1996*, matters relating to the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia.

1. In performing its functions in relation to this reference, the Commission will consider:

(a) relevant existing and proposed Commonwealth, State and Territory laws and practices

(b) other recent reviews of the *Privacy Act 1988*

(c) current and emerging international law and obligations in this area

(d) privacy regimes, developments and trends in other jurisdictions

(e) any relevant constitutional issue

(f) the need of individuals for privacy protection in an evolving technological environment

(g) the desirability of minimising the regulatory burden on business in this area, and

(h) any other related matter.

2. The Commission will identify and consult with relevant stakeholders, including the Office of the Federal Privacy Commissioner, relevant State and Territory bodies and the Australian business community, and ensure widespread public consultation.

3. The Commission is to report no later than 31 March 2008.

Dated 30th January 2006

[signed]

Philip Ruddock

Attorney-General

List of Participants

Australian Law Reform Commission

Division

The Division of the ALRC constituted under the *Australian Law Reform Commission Act 1996* (Cth) for the purposes of this Inquiry comprises the following:

Professor David Weisbrot (President)
Professor Les McCrimmon (Commissioner in-charge)
Professor Rosalind Croucher (Commissioner)
Justice Robert French (part-time Commissioner)
Justice Susan Kenny (part-time Commissioner)
Justice Susan Kiefel (part-time Commissioner) (until August 2007)

Senior Legal Officers

Carolyn Adams
Bruce Alston
Jonathan Dobinson

Legal Officers

Lisa Eckstein (from August 2007)
Althea Gibson (until March 2007)
Lauren Jamieson
Huette Lam
Erin Mackay (from March 2007)
Edward Santow
Peter Turner (until August 2006)

Research Manager

Lani Blackman

Librarian

Carolyn Kearney

Project Assistant

Tina O'Brien

Legal Interns

Megan Caristo
Justin Carter
Elizabeth Crook
Joash Dache
Maggie Fung
Dawnie Lam
Robert Mullins
Danni Nicholas-Sexon
Elnaz Nikibin
Michael Ostroff
Christina Raymond
Fiona Roughley
Keelyann Thomson
Christina Trahanas
Teneille Steptoe
Michelle Tse
Jocelyn Williams
SooJin Yoon

Advisory Committee Members

Dr Bridget Bainbridge, National E-Health Transition Authority
Ms Robin Banks, Public Interest Advocacy Centre
Mr Paul Chadwick, Consultant (formerly Victorian Privacy Commissioner) (until January 2007)
Ms Karen Curtis, Privacy Commissioner (Cth)
Mr Peter Ford, Privacy, Security and Telecommunications Consultant
Mr Ian Gilbert, Australian Bankers' Association
Mr Duncan Giles, Freehills Solicitors
Professor Margaret Jackson, School of Accounting & Law, RMIT University
Ms Helen Lewin, Telstra Corporation
Associate Professor Roger Magnusson, Faculty of Law, University of Sydney
Associate Professor Moira Paterson, Faculty of Law, Monash University
Ms Joan Sheedy, Australian Government Attorney-General's Department
Mr Peter Shoyer, Executive Director of Court Support & Independant Offices NT
Professor Colin Thomson, National Health and Medical Research Council
Mr Nigel Waters, Pacific Privacy Consulting
Ms Beth Wilson, Health Services Commissioner (Vic)
Ms Sue Vardon, Department for Families & Communities (SA)

Credit Reporting Advisory Sub–Committee

Ms Carolyn Bond, Consumer Action Law Centre
Ms Christine Christian, Dun and Bradstreet Pty Ltd

Ms Karen Cox, Consumer Credit Legal Centre (NSW)
Mr Ian Gilbert, Australian Bankers' Association
Ms Helen Gordon, Australian Finance Conference
Mr David Grafton, Commonwealth Bank of Australia
Ms Loretta Kreet, Legal Aid Queensland
Mr Andrew Want, Veda Advantage
Mr Nigel Waters, Pacific Privacy Consulting
Ms Kerstin Wijeyewardene, Treasury (Cth)

Developing Technology Advisory Sub–Committee

Mr Paul Budde, Managing Director, BuddeComm
Professor William Caelli, Director Information Assurance, International Information Security Consultants Pty Ltd and Faculty of Information Technology, QUT
Mr Chris Cheah, Australian Communications and Media Authority
Professor Peter Croll, Professor of Software Engineering, Faculty of Information Technology, QUT
Mr Malcolm Crompton, Information Integrity Solutions Pty Ltd
Professor Graham Greenleaf, Faculty of Law, University of New South Wales
Professor Margaret Jackson, School of Accounting and Law, RMIT University
David Jonas, Convergence e-Business Solutions Pty Ltd
Mr Greg Stone, National Technology Officer, Microsoft Pty Ltd
Mr Martin Stewart Weeks, Internet Business Solutions Group, Cisco Systems Australia Pty Ltd
Professor Michael Wagner, National Centre for Biometric Studies, University of Canberra
Mr Stephen Wilson, Lockstep Consulting

Health Advisory Sub–Committee

Ms Amanda Adrian, Australian Nursing Federation
Ms Melanie Cantwell, Consumers' Health Forum of Australia Inc
Professor David Hill, The Cancer Council (Vic)
Ms Anna Johnston, Australian Privacy Foundation
Dr Graeme Miller, Family Medicine Research Centre
Ms Julia Nesbitt, Australian Medical Association
Professor Margaret Otlowski, Faculty of Law, University of Tasmania
Ms Dianne Scott, Department of Human Services (Vic)
Dr Heather Wellington, Peter MacCallum Cancer Centre

List of Proposals and Questions

Part A—Introduction

1. Introduction to the Inquiry

Proposal 1–1 The Office of the Privacy Commissioner should, either on its own motion or where approached in appropriate cases, encourage and assist agencies and organisations, in conjunction with Indigenous and other ethnic groups in Australia, to create publicly available protocols that adequately respond to the particular privacy needs of those groups.

3. The *Privacy Act*

Proposal 3–1 The *Privacy Act* should provide for the making of regulations that modify the operation of the proposed Unified Privacy Principles (UPPs) to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.

Proposal 3–2 The *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity. For example, the Information Privacy Principles and the National Privacy Principles should be consolidated into a set of UPPs; the exemptions should be clarified and grouped together in a separate part of the Act; and the Act should be restructured and renumbered.

Proposal 3–3 If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, the name of the Act should remain the same. If the Act is not amended in this way, however, the *Privacy Act* should be renamed the *Privacy and Personal Information Act*.

Proposal 3–4 The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be to:

(a) implement Australia's obligations at international law in relation to privacy;

(b) promote the protection of individual privacy;

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;

(d) establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy; and

(g) provide the basis for nationally consistent regulation of privacy.

Proposal 3–5 (a) The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

(b) The Explanatory Memorandum of the amending legislation should make clear that an individual is 'reasonably identifiable' when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.

(c) The Office of the Privacy Commissioner should provide guidance on the meaning of 'identified or reasonably identifiable'.

Proposal 3–6 The definition of 'sensitive information' in the *Privacy Act* should be amended to include: (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information.

Proposal 3–7 The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.

Proposal 3–8 The definition of 'record' in the *Privacy Act* should be amended in part to include: (a) a document; and (b) information stored in electronic or other forms.

Proposal 3–9 The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

Proposal 3–10 The personal information of deceased individuals held by agencies should continue to be regulated by the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth).

Proposal 3–11 The *Privacy Act* should be amended to include a new Part dealing with the personal information of individuals who have been dead for 30 years or less

where the information is held by an organisation. The new Part should provide as follows:

(a) Use and disclosure

Organisations should be required to use or disclose the personal information of deceased individuals in accordance with the proposed 'Use and Disclosure' principle in the UPPs. Where the principle requires consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to consider providing third parties with access to the personal information of deceased individuals in accordance with the access elements of the proposed 'Access and Correction' principle in the UPPs. Organisations should be required to consider in each case whether providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data quality

Organisations should be required to ensure that the personal information of deceased individuals is, with reference to a use or disclosure permitted under the UPPs, accurate, complete, up-to-date and relevant before they use or disclose the information.

(d) Data security

Organisations should be required to take reasonable steps to protect the personal information of deceased individuals from misuse and loss and from unauthorised access, modification or disclosure.

Organisations should be required to take reasonable steps to destroy or render personal information of deceased individuals non-identifiable if it is no longer needed for any purpose permitted under the proposed UPPs.

Organisations should be required to take reasonable steps to ensure that personal information of deceased individuals they disclose to a person pursuant to contract, or otherwise in connection with the provision of a service, is protected from being used or disclosed by that person otherwise than in accordance with the *Privacy Act*.

Proposal 3–12 The proposed provisions dealing with the use or disclosure of personal information of deceased individuals should make clear that it is reasonable for an organisation to use or disclose genetic information to a genetic relative of a

deceased individual where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. Any use or disclosure of genetic information of deceased individuals should be in accordance with rules issued by the Privacy Commissioner.

Proposal 3–13 Breach of the proposed provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner alleging an interference with the privacy of a deceased individual:

(a) in relation to an alleged breach of the use and disclosure, data quality or data security provisions, the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner or legal personal representative; and

(b) in relation to an alleged breach of the access provision, any person who has made a request for access to the personal information of a deceased individual.

4. Achieving National Consistency

Proposal 4–1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic);

(c) *Health Records (Privacy and Access) Act 1997* (ACT); and

(d) any other laws prescribed in the regulations.

Proposal 4–2 States and territories with information privacy legislation that purports to apply to private sector organisations should amend that legislation so that it is no longer expressed to apply to private sector organisations.

Proposal 4–3 The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the legislation. The Australian Government, in consultation with state and territory governments, should develop a list of 'non-excluded matters', for example matters such as:

(a) reporting for child protection purposes;

(b) reporting for public health purposes; and

(c) the handling of personal information by state and territory government contractors.

Proposal 4–4 The states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector that:

(a) applies the proposed Unified Privacy Principles (UPPs) and the proposed *Privacy (Health Information) Regulations* as in force under the *Privacy Act* from time to time; and

(b) includes at a minimum:

(i) relevant definitions used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information');

(ii) provisions allowing public interest determinations and temporary public interest determinations;

(iii) provisions relating to state and territory incorporated bodies (including statutory corporations);

(iv) provisions relating to state and territory government contracts; and

(v) provisions relating to data breach notification.

The legislation also should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

Proposal 4–5 The Australian Government should initiate a review in five years to consider whether the proposed Commonwealth-state cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors.

Proposal 4–6 To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the proposed:

(a) UPPs must be approved by SCAG; and

(b) Privacy *(Health Information) Regulations* must be approved by SCAG, in consultation with the Australian Health Ministers' Advisory Council (AHMAC).

The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

Proposal 4–7 The Standing Committee of Attorneys-General should be assisted by an expert advisory committee to:

(a) provide advice in relation to the amendment of the proposed UPPs and *Privacy (Health Information) Regulations*;

(b) address issues related to national consistency such as the scrutiny of federal, state and territory bills that may adversely impact on national consistency in the regulation of personal information; and

(c) address issues related to the enforcement of privacy laws, including information sharing between privacy regulators and cooperative arrangements for enforcement.

Appointments to the expert advisory committee should ensure a balanced and broad-based range of expertise, experience and perspectives relevant to the regulation of personal information. The appointments process should involve consultation with state and territory governments, business, privacy and consumer advocates and other stakeholders.

5. Protection of a Right to Personal Privacy

Proposal 5–1 The *Privacy Act* should be amended to provide for a statutory cause of action for invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, an invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

Proposal 5–2 The *Privacy Act* should provide that, in determining what is considered 'private' for the purpose of establishing liability under the proposed statutory cause of action, a plaintiff must show that in all the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities.

Proposal 5–3 The *Privacy Act* should provide that:

(a) only natural persons should be allowed to bring an action under the *Privacy Act* for invasion of privacy;

(b) the action is actionable without proof of damage; and

(c) the action is restricted to intentional or reckless acts on the part of the defendant.

Proposal 5–4 The Office of the Privacy Commissioner should provide information to the public concerning the proposed statutory cause of action for invasion of privacy.

Proposal 5–5 The range of defences to the proposed statutory cause of action for invasion of privacy provided for in the *Privacy Act* should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or specifically authorised by or under law;

(c) information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

(d) disclosure of the information was, under the law of defamation, privileged.

Question 5–1 In addition to the defences listed in Proposal 5–5, are there any other defences that should apply to the proposed statutory cause of action for invasion of privacy?

Proposal 5–6 To address an invasion of privacy, the court should be empowered by the *Privacy Act* to choose the remedy that is most appropriate in all the circumstances, free from the jurisdictional constraints that may apply to that remedy in

the general law. For example, the court should be empowered to grant any one or more of the following:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the defendant to apologise to the plaintiff;

(e) a correction order;

(f) an order for the delivery up and destruction of material;

(g) a declaration; and

(h) other remedies or orders that the court thinks appropriate in the circumstances.

Proposal 5–7 Until such time as the states and territories enact uniform legislation, the state and territory public sectors should be subject to the proposed statutory cause of action for invasion of privacy in the *Privacy Act*.

Part B—Developing Technology

7. Accommodating Developing Technology in a Regulatory Framework

Proposal 7–1 The *Privacy Act* should be technologically neutral.

Proposal 7–2 The *Privacy Act* should be amended to empower the Minister responsible for the *Privacy Act*, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.

Proposal 7–3 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations.

Proposal 7–4 The Office of the Privacy Commissioner should educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed.

Proposal 7–5 The Office of the Privacy Commissioner should provide guidance in relation to technologies that impact on privacy (including, for example, guidance for

use of RFID or data collecting software such as 'cookies'). Where appropriate, this guidance should incorporate relevant local and international standards. The guidance should address:

(a) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';

(b) when the use of a certain technology will require, under the proposed 'Specific Notification' principle, agencies and organisations to notify individuals at or before the time of collection of personal information;

(c) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometrics systems);

(d) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information held in an intelligible form (for example, what biometric information is held about an individual when the information is held as an algorithm); and

(e) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

Proposal 7–6 The Office of the Privacy Commissioner should provide guidance to organisations on the privacy implications of data-matching.

8. Individuals, the Internet and Generally Available Publications

Question 8–1 Should the online content regulation scheme set out in the *Broadcasting Services Act 1992* (Cth), and in particular the ability to issue take down notices, be expanded beyond the *National Classification Code* and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take down notice should be issued? What is the appropriate body to deal with a complaint and issue the take down notice?

Proposal 8–1 The Office of the Privacy Commissioner should provide guidance that relates to generally available publications in an electronic form. This guidance should:

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out certain factors that agencies and organisations should consider before publishing personal information in an electronic form (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

(c) set out the requirements in the proposed Unified Privacy Principles with which agencies and organisations need to comply when collecting personal information from generally available publications for inclusion in a record or another generally available publication (for example, when a reasonable person would expect to be notified of the fact and circumstances of collection).

Part C—Interaction, Inconsistency and Fragmentation

11. The Costs of Inconsistency and Fragmentation

Proposal 11–1 The Office of the Privacy Commissioner should provide further guidance to agencies and organisations on privacy requirements affecting information sharing.

Proposal 11–2 Agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information; and where appropriate, publish other documents (including memoranda of understanding and ministerial agreements) relating to the sharing of personal information.

Proposal 11–3 The Australian Government should convene an inter-agency working group of senior officers to identify circumstances where it would be appropriate to share or streamline the sharing of personal information among Australian Government agencies.

Proposal 11–4 The Australian Government, in consultation with: state and territory governments, intelligence agencies, law enforcement agencies, and accountability bodies (including the Office of the Privacy Commissioner; the Inspector-General of Intelligence and Security; the Australian Commission for Law Enforcement Integrity; state and territory privacy commissioners and agencies with responsibility for privacy regulation; and federal, state and territory ombudsmen), should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memoranda of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

Question 11–1 Are the definitions of 'contracted service provider' and 'State contract' under the *Privacy Act* adequate? For example, do they cover all the types of activities that organisations might perform on behalf of agencies?

12. Federal Information Laws

Proposal 12–1 The Australian Government and state and territory governments should ensure the consistency of definitions and key terms (for example, 'personal information', 'sensitive information' and 'health information') in federal, state and territory legislation that regulates the handling of personal information.

Proposal 12–2 Section 41(1) of the *Freedom of Information Act 1982* (Cth) should be amended to provide that a document is exempt if it:

(a) contains personal information, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle and disclosure would not, on balance, be in the public interest; or

(b) contains personal information of a deceased individual, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle (but where the principle would require consent the agency must consider whether the proposed disclosure would involve the unreasonable disclosure of personal information about any individual including the deceased individual) and disclosure would not, on balance, be in the public interest.

Proposal 12–3 'Personal information' should be defined in the *Freedom of Information Act 1982* (Cth) as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

Proposal 12–4 The *Freedom of Information Act 1982* (Cth) should be amended to require that the body that is primarily responsible for administration of the Act is to:

(a) develop and publish guidelines on the interpretation and application of s 41;

(b) consult with the Office of the Privacy Commissioner before issuing guidelines on the interpretation and application of s 41.

Proposal 12–5 The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act 1982* (Cth) is a disclosure that is required or authorised for the purposes of the proposed 'Use and Disclosure' principle under the *Privacy Act*.

Proposal 12–6 The *Privacy Act* should be amended to provide a new Part dealing with access to, and correction of, personal information held by an agency.

Proposal 12–7 The *Freedom of Information Act 1982* (Cth) should be amended to:

(a) provide that an individual's right to access or correct his or her own personal information is dealt with under the *Privacy Act*; and

(b) repeal Part V of the Act.

Proposal 12–8 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that:

(a) if an agency holds personal information about an individual the agency must, if requested by the individual, provide the individual with access to the information, subject to a number of exceptions under the Part;

(b) where an individual is given access to personal information, the individual must be advised that he or she may request the correction of that information;

(c) where an agency is not required to provide the individual with access to personal information because of an exception, the agency must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties; and

(d) nothing in the Part is intended to prevent or discourage agencies from publishing or giving access to personal information, otherwise than as required by the Part, where they can do so properly or are required to do so by law.

Question 12–1 What exceptions should apply to the general provision granting an individual the right to access his or her own personal information held by an agency? For example, should the exceptions mirror the provisions in Part IV of the *Freedom of Information Act 1982* (Cth) or should another set of exceptions apply?

Proposal 12–9 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that, if an agency holds personal information about an individual, the agency must:

(a) if requested by the individual, take such steps to correct (by way of making appropriate corrections, deletions or additions) the information as are, in the circumstances, reasonable to ensure that the information is, with reference to a purpose of collection permitted by the proposed Unified Privacy Principles, accurate, complete, up-to-date, relevant and not misleading;

(b) where the agency has taken the steps outlined in (a) above, if requested to do so by the individual, and provided such notification would be practicable in the circumstances, notify any other entities to whom the personal information has already been disclosed.

Proposal 12–10 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that where an agency decides not to correct the personal information of an individual, and the individual requests the agency to annotate the personal information with a statement by the individual claiming that the information is not accurate, complete, up-to-date, relevant, or is misleading, the agency must take reasonable steps to do so.

Proposal 12–11 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should set out a process for dealing with a request to access or correct personal information that addresses:

(a) the requirements for making an application for correction or annotation of personal information;

(b) time periods for processing a request to access or correct personal information;

(c) the transfer of a request to access or correct personal information to another agency in certain circumstances (for example, when a document is not in the possession of an agency but is, to the knowledge of that agency, in the possession of another agency);

(d) how personal information is to be made available to the individual (including by giving the individual a reasonable opportunity to inspect the records, or by providing a copy of the record, by giving a summary of the contents of the record, or by providing oral information about the contents of the record);

(e) how corrections are to be made (including by additions and deletions);

(f) the deletion of excepted matter or irrelevant material;

(g) the persons authorised to make a decision on behalf of an agency in relation to a request to access or correct personal information;

(h) when a request for access to personal information may be refused by an agency (for example, when it would substantially and unreasonably divert the resources of the agency from its other operations, or in the case of a minister, would substantially and unreasonably interfere with the performance of the minister's functions); and

(i) the provision of reasons for a decision to deny a request to access or correct personal information.

Proposal 12–12 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide for:

(a) internal review by an agency of a decision made under the Part;

(b) review by the Administrative Appeals Tribunal of a decision made under the Part (including the power to make an order for compensation); and

(c) complaints to the Commonwealth Ombudsman.

Proposal 12–13 The Office of the Privacy Commissioner should issue guidelines on access to, and correction of, records containing personal information held by an agency.

Question 12–2 Should the Office of the Privacy Commissioner's complaint-handling, investigative and reporting functions be exempt under the *Freedom of Information Act 1982* (Cth)?

Proposal 12–14 Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

13. Required or Authorised by or under Law

Question 13–1 Should the definition of a 'law' for the purposes of determining when an act or practice is required or specifically authorised by or under a law include:

(a) a common law or equitable duty;

(b) an order of a court or tribunal;

(c) documents that are given the force of law by an Act of Parliament, such as industrial awards; and

(d) statutory instruments such as a Local Environmental Plan made under a planning law?

Question 13–2 Should a list be compiled of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*? If so, should the list have the force of law? Should it be comprehensive or indicative? What body should be responsible for compiling and updating the list?

Proposal 13–1 If the exemption that applies to registered political parties and political acts and practices is not removed, the *Commonwealth Electoral Act 1918* (Cth) should be amended to provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information in relation to the electoral roll and certified lists of voters must take reasonable steps to:

(a) protect the information from misuse and loss and from unauthorised access, modification or disclosure; and

(b) destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.

Proposal 13–2 The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

Proposal 13–3 The review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), the regulations and the Anti-Money Laundering and Counter-Terrorism Financing Rules under s 251 of the Act should consider, in particular, whether:

(a) reporting entities and designated agencies are appropriately handling personal information under the legislation;

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years; and

(d) it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.

Proposal 13–4 The *Anti-Money Laundering* and *Counter-Terrorism Financing Act 2006* (Cth) should be amended to provide that state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the Act be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act.*

14. Interaction with State and Territory Laws

Proposal 14–1 The *Privacy Act* should be amended to provide that when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies, the Australian Government agency should ensure that a memorandum of understanding is in place so that the intergovernmental body and its members do not act, or engage in a practice, that would breach the Act.

Part D—The Privacy Principles

15. Structural Reform of the Privacy Principles

Proposal 15–1 The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

(a) the obligations in the privacy principles generally should be expressed as high level principles;

(b) the privacy principles should be simple, clear and easy to understand and apply; and

(c) the privacy principles should impose reasonable obligations on agencies and organisations.

Proposal 15–2 The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles—the Unified Privacy Principles (UPPs)—that would be generally applicable to agencies and organisations, subject to such exceptions as required.

Proposal 15–3 The proposed UPPs should apply to information privacy except to the extent that:

(a) the *Privacy Act* or another piece of Commonwealth primary legislation imposes different or more specific requirements in a particular context; or

(b) subordinate legislation under the *Privacy Act* imposes different or more specific requirements in a particular context.

Proposal 15–4 The National Privacy Principles should provide the general template in drafting and structuring the proposed UPPs.

16. Consent

Proposal 16–1 The Office of the Privacy Commissioner should provide further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should: (a) cover consent as it applies in various contexts; and (b) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

17. Anonymity and Pseudonymity

Proposal 17–1 The proposed Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that sets out the requirements on agencies and organisations in respect of anonymous and pseudonymous transactions with individuals.

Proposal 17–2 The proposed 'Anonymity and Pseudonymity' principle should include a pseudonymity requirement that when an individual is transacting with an agency or organisation, the agency or organisation must give the individual the option of identifying himself or herself by a pseudonym. This requirement is limited to circumstances where providing this option is lawful, practicable and not misleading.

Proposal 17–3 The proposed 'Anonymity and Pseudonymity' principle should provide that, subject to the relevant qualifications in the principle, an agency or organisation is required to give individuals the clear option to transact anonymously or pseudonymously.

Proposal 17–4 The Office of the Privacy Commissioner should provide guidance to agencies and organisations on: (a) when it is and is not lawful and practicable to give individuals the option to transact anonymously or pseudonymously; (b) when it would be misleading for an individual to transact pseudonymously with an agency or organisation; and (c) what is involved in providing a clear option to transact anonymously or pseudonymously.

18. Collection

Proposal 18–1 (a) The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

(b) The Office of the Privacy Commissioner should provide guidance to clarify when it would not be reasonable and practicable to collect such information from the individual concerned.

Proposal 18–2 The 'Collection' principle in the proposed UPPs should provide that, where an agency or organisation receives unsolicited personal information, it must either: (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

Proposal 18–3 The 'Collection' principle in the proposed UPPs should provide that an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.

19. Sensitive Information

Proposal 19–1 The proposed Unified Privacy Principles should set out the requirements on agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*. These requirements should be located in the proposed 'Collection' principle.

Proposal 19–2 The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or specifically authorised by or under law.

Proposal 19–3 The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent.

Question 19–1 Should the proposed sensitive information provisions provide that sensitive information can be collected where all of the following conditions apply:

(a) the individual is incapable of giving consent;

(b) the collection is necessary to provide an essential service for the benefit of the individual; and

(c) the collection would be reasonable in all the circumstances?

20. Specific Notification

Proposal 20–1 The proposed Unified Privacy Principles should contain a principle called 'Specific Notification' that sets out the requirements on agencies and organisations to provide specific notification to an individual of particular matters relating to the collection and handling of personal information about the individual.

Proposal 20–2 The proposed 'Specific Notification' principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

(a) fact and circumstances of collection (for example, how, when and from where the information was collected);

(b) identity and contact details of the agency or organisation;

(c) fact that the individual is able to gain access to the information;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and

(g) avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

This requirement should only apply: (1) in circumstances where a reasonable person would expect to be notified; (2) except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and (3) subject to any other relevant exceptions.

Proposal 20–3 The Office of the Privacy Commissioner should provide guidance to assist agencies and organisations in ensuring that individuals are properly informed of the persons to whom their personal information is likely to be disclosed.

Proposal 20–4 An agency should be required to notify an individual of the matters listed in the proposed 'Specific Notification' principle, except to the extent that the agency is required or specifically authorised by or under law not to make the individual aware of such matters.

Proposal 20–5 (a) The proposed 'Specific Notification' principle should provide that where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of:

(i) the matters listed in Proposal 20–2; and

(ii) on request by the individual, the source of the information.

(b) This requirement should only apply:

(i) in circumstances where a reasonable person would expect to be notified;

(ii) except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and

(iii) in the case of an agency, except to the extent that it is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.

Proposal 20–6 The Office of the Privacy Commissioner should provide guidance on the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information about the individual from a source other than the individual concerned.

Proposal 20–7 The Office of the Privacy Commissioner should provide guidance on the meaning of the term 'reasonable steps' in the context of an agency's or organisation's obligations to fulfil its notification requirements under the proposed 'Specific Notification' principle.

21. Openness

Proposal 21–1 The proposed Unified Privacy Principles should contain a principle called 'Openness' that sets out the requirements on an agency or organisation to operate openly and transparently by providing general notification in a Privacy Policy of how it manages personal information and how personal information is collected, held, used and disclosed by it.

Proposal 21–2 The Privacy Policy in the proposed 'Openness' principle should set out an agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation;

(e) the types of individuals about whom records are kept;

(f) the period for which each type of record is kept; and

(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.

Proposal 21–3 The Office of the Privacy Commissioner should issue guidance on how agencies and organisations can comply with their obligations in the proposed 'Openness' principle to produce and make available a Privacy Policy.

Proposal 21–4 An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the proposed 'Openness' principle, available without charge to an individual: (a) electronically (for example, on its website, if it possesses one); and (b) in hard copy, on request.

Proposal 21–5 The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

22. Use and Disclosure

Proposal 22–1 The proposed Unified Privacy Principles should contain a principle called 'Use and Disclosure' that sets out the requirements on agencies and organisations in respect of the use or disclosure of personal information for a purpose other than the primary purpose of collecting the information.

Proposal 22–2 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the:

(a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.

Proposal 22–3 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the agency or organisation reasonably believes that the use or

disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.

Question 22–1 Should the proposed 'Use and Disclosure' principle contain an exception allowing an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of collection where this is 'required or *specifically* authorised by or under law' instead of simply 'required or authorised by or under law'?

23. Direct Marketing

Proposal 23–1 The proposed Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' privacy principle. This principle should be called 'Direct Marketing' and it should apply irrespective of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing.

Question 23–1 Should agencies be subject to the proposed 'Direct Marketing' principle? If so, should any exceptions or exemptions apply specifically to agencies?

Proposal 23–2 The proposed 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.

Proposal 23–3 The proposed 'Direct Marketing' principle should require organisations to present individuals with a simple means to opt out of receiving direct marketing communications.

Proposal 23–4 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must comply, within a reasonable time, with an individual's request not to receive direct marketing communications.

Proposal 23–5 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must, when requested by an individual to whom it has sent direct marketing communications, take reasonable steps to advise the individual from where it acquired the individual's personal information.

Proposal 23–6 The Office of the Privacy Commissioner should issue guidance to organisations involved in direct marketing, which should:

(a) highlight their obligation to maintain the quality of any database they hold containing personal information and assists them in achieving this requirement; and

(b) clarify their obligations under the *Privacy Act* in dealing with particularly vulnerable people, such as elderly individuals and individuals aged 14 and under.

24. Data Quality

Proposal 24–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Data Quality' that applies to agencies and organisations.

Proposal 24–2 The proposed 'Data Quality' principle should require an agency or organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the proposed UPPs, accurate, complete, up-to-date and relevant.

25. Data Security

Proposal 25–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Data Security' that applies to agencies and organisations.

Proposal 25–2 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

Proposal 25–3 The Office of the Privacy Commissioner should provide guidance about the meaning of the term 'reasonable steps' in the context of the proposed 'Data Security' principle. Matters that could be dealt with in this guidance include:

(a) the inclusion of contractual provisions binding a contracted service provider of an agency or organisation to handle personal information consistently with the UPPs;

(b) technological developments in this area and particularly in relation to relevant encryption standards; and

(c) the importance of training staff adequately as to the steps they should take to protect personal information.

Proposal 25–4 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs.

Proposal 25–5 The Office of the Privacy Commissioner should provide guidance about when it is appropriate for an agency or organisation to destroy or render non-identifiable personal information that is no longer needed for a purpose permitted under the UPPs. This guidance should cover, among other things:

(a) personal information that forms part of a historical record;

(b) personal information, or a record of personal information, that may need to be preserved, in some form, for the purpose of future dispute resolution; and

(c) the interaction between the UPPs and legislative records retention requirements.

Proposal 25–6 The Office of the Privacy Commissioner should provide guidance about what is required of an agency or organisation to destroy or render non-identifiable personal information, particularly when that information is held or stored in an electronic form.

26. Access and Correction

Proposal 26–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Access and Correction' that:

(a) sets out the requirements that apply to organisations in respect of personal information that is held by organisations; and

(b) contains a note stating that the provisions dealing with access to, and correction of, personal information held by agencies are located in a separate Part of the *Privacy Act*.

Proposal 26–2 (a) The proposed 'Access and Correction' principle should provide that, where an organisation is not required to provide an individual with access to his or her personal information because of an exception to the general provision granting a right of access, the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, that would allow for sufficient access to meet the needs of both parties.

(b) The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable steps' in this context, making clear, for instance, that an organisation need not take any steps where this would undermine a lawful reason for denying a request for access in the first place.

Proposal 26–3 The proposed 'Access and Correction' principle should provide that an organisation must respond within a reasonable time to a request from an individual for access to personal information held by the organisation. The Office of

the Privacy Commissioner should provide guidance about the meaning of 'reasonable time' in this context.

Proposal 26–4 The proposed 'Access and Correction' principle should provide that where, in accordance with this principle, an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed prior to correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances.

Proposal 26–5 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual that the individual wishes to have corrected or annotated, the individual should seek to establish that the personal information held by the organisation is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant.

Proposal 26–6 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to that information to the individual to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.

27. Identifiers

Proposal 27–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Identifiers' that applies to agencies and organisations. As a consequence, s 100(2) and (3) of the *Privacy Act* should be amended to apply also to agencies.

Proposal 27–2 The proposed 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or any other particular that:

(a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or

(b) is determined to be an identifier by the Office of the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Proposal 27–3 The proposed 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth).

Proposal 27–4 The proposed 'Identifiers' principle should regulate the use by agencies and organisations of identifiers that are assigned by state and territory agencies.

Question 27–1 Should the *Privacy Act* regulate the assignment of identifiers by agencies, organisations or both? If so, what requirements should apply and should these requirements be located in the proposed UPPs or elsewhere?

Proposal 27–5 Before the introduction by agencies of any unique multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment.

Proposal 27–6 The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the *Tax File Number Guidelines* issued under s 17 of the *Privacy Act*.

28. Transborder Data Flows

Proposal 28–1 The *Privacy Act* should be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.

Proposal 28–2 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Transborder Data Flows' that applies to agencies and organisations.

Proposal 28–3 The proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia if the transfer is necessary for one or more of the following by or on behalf of an enforcement body:

(a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(b) the enforcement of laws relating to the confiscation of the proceeds of crime;

(c) the protection of the public revenue;

(d) the prevention, detection, investigation or remedying of seriously improper conduct or proscribed conduct;

(e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(f) extradition and mutual assistance.

Question 28–1 Should the *Privacy Act* provide that for the purposes of the proposed 'Transborder Data Flows' principle, a 'transfer':

(a) includes where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia; and

(b) excludes the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia?

Proposal 28–4 Subject to Proposal 28–3, the proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia only if at least one of the following conditions is met:

(a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs; or

(b) the individual consents to the transfer; or

(c) the agency or organisation continues to be liable for any breaches of the proposed UPPs; and

    (i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;

    (ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

    (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

    (iv) all of the following apply: the transfer is for the benefit of the individual; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

(v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.

Proposal 28–5 The proposed 'Use and Disclosure' principle should contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

Proposal 28–6 The proposed 'Transborder Data Flows' principle should contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

Proposal 28–7 Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, this transfer will be subject to the proposed 'Transborder Data Flows' principle.

Proposal 28–8 The Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed UPPs.

Proposal 28–9 The Office of the Privacy Commissioner should develop and publish guidance on the proposed 'Transborder Data Flows' principle, including guidance on:

(a) when personal information may become available to a foreign government;

(b) outsourcing government services to organisations outside Australia;

(c) the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal information;

(d) when a transfer of personal information is 'for the benefit' or 'in the interests of' the individual concerned; and

(e) what constitute 'reasonable steps' to ensure the information it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the proposed UPPs.

Proposal 28–10 The Privacy Policy of an agency or organisation, referred to in the proposed 'Openness' principle, should set out whether personal information may be transferred outside Australia.

Question 28–2 Would the use of trustmarks be an effective method of promoting compliance with, and enforcement of, the *Privacy Act* and other international privacy regimes? If so, should they be provided for under the *Privacy Act*?

Part E—Exemptions

30. Overview—Exemptions from the *Privacy Act 1988* (Cth)

Proposal 30–1 The *Privacy Act* should be amended to group together in a separate part of the Act exemptions for certain categories of entities or types of acts and practices.

Proposal 30–2 The *Privacy Act* should be amended to set out in a schedule to the Act exemptions for specific, named entities. The schedule should distinguish between entities that are completely exempt and those that are partially exempt from the Privacy Act. For those entities that are partially exempt, the schedule should specify those acts and practices that are exempt.

31. Defence and Intelligence Agencies

Proposal 31–1 The privacy rules and guidelines, which relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, Australian Security Intelligence Service, Defence Imagery and Geospatial Organisation, Defence Intelligence Organisation, Defence Signals Directorate and Office of National Assessments, should be amended to include consistent rules and guidelines relating to:

(a) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of the incident and measures taken to protect the privacy of the Australian person);

(b) the accuracy of personal information; and

(c) the storage and security of personal information.

Proposal 31–2 Section 15 of the *Intelligence Services Act 2001* (Cth) should be amended to provide that:

(a) the responsible minister in relation to the Defence Intelligence Organisation is required to make written rules regulating the communication and retention by the Defence Intelligence Organisation of intelligence information concerning Australian persons; and

(b) before making rules to protect the privacy of Australian persons, the ministers responsible for the Australian Security Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Defence Intelligence Organisation should consult with the Office of the Privacy Commissioner.

Proposal 31–3 The *Office of National Assessments Act 1977* (Cth) should be amended to provide that:

(a) the responsible minister in relation to the Office of National Assessments (ONA) is required to make written rules regulating the communication and retention by the ONA of intelligence information concerning Australian persons; and

(b) before making rules to protect the privacy of Australian persons, the minister responsible for the ONA should consult with the Office of the Privacy Commissioner.

Proposal 31–4 Section 8A of the *Australian Security* and *Intelligence Organisation Act 1979* (Cth) should be amended to provide that, before making rules to protect the privacy of Australian persons, the responsible minister should consult with the Office of the Privacy Commissioner.

Proposal 31–5 The privacy rules and guidelines referred to in Proposal 31–1 should be made available electronically to the public; for example, on the websites of those agencies.

Proposal 31–6 The *Privacy Act* should be amended to apply to the Inspector-General of Intelligence and Security (IGIS) in respect of the administrative operations of that office.

Proposal 31–7 The Inspector-General of Intelligence and Security, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by IGIS is protected adequately.

32. Federal Courts and Tribunals

Proposal 32–1 Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.

Question 32–1 Should the *Privacy Act* be amended to provide that federal tribunals are exempt from the operation of the Act in respect of their adjudicative functions? If so, what should be the scope of ‘adjudicative functions’?

33. Exempt Agencies under the *Freedom of Information Act 1982* (Cth)

Proposal 33–1 The *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Fair Pay Commission under s 7(1) of the Act.

Proposal 33–2 The following agencies listed in Schedule 2 Part I Division 1 and Part II Division 1 of the *Freedom of Information Act 1982* (Cth) should be required to demonstrate to the Attorney-General of Australia that they warrant exemption from the operation of the *Privacy Act*:

(a) Aboriginal Land Councils and Land Trusts;

(b) Auditor-General;

(c) National Workplace Relations Consultative Council;

(d) Department of the Treasury;

(e) Reserve Bank of Australia;

(f) Export and Finance Insurance Corporation;

(g) Australian Communications and Media Authority;

(h) Classification Board;

(i) Classification Review Board;

(j) Australian Trade Commission; and

(k) National Health and Medical Research Council.

The Australian Government should remove the exemption from the operation of the *Privacy Act* for any of these agencies that, within 12 months, do not make an adequate case for retaining their exempt status.

Proposal 33–3 The *Privacy Act* should be amended to remove the exemption of the Australian Broadcasting Corporation and the Special Broadcasting Service listed in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth).

34. Other Public Sector Exemptions

Proposal 34–1 The Attorney-General's Department, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for royal commissions to assist in ensuring that the personal information they handle is protected adequately.

Proposal 34–2 The *Privacy Act* should be amended to remove the exemption that applies to the Australian Crime Commission and the Board of the Australian Crime Commission by repealing s 7(1)(a)(iv), (h) and 7(2) of the Act.

Proposal 34–3 The *Privacy Act* should be amended to apply to the Integrity Commissioner in respect of the administrative operations of his or her office.

Proposal 34–4 The Integrity Commissioner, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity is protected adequately.

Question 34–1 Should the *Privacy Act* be amended to set out, in the form of an exemption, the range of circumstances in which agencies that perform law enforcement functions, such as the Australian Federal Police and the Australian Crime Commission, are not required to comply with specific privacy principles?

Question 34–2 Should the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary Services continue to be exempt from the operation of the *Privacy Act*? If so, what should be the scope of the exemption?

Proposal 34–5 Subject to Proposal 4–4 (states and territories to enact legislation applying the proposed Unified Privacy Principles and *Privacy (Health Information) Regulations*), the *Privacy Act* should be amended to:

(a) apply to all state and territory incorporated bodies, including statutory corporations, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of the relevant obligations in the *Privacy Act*; and

(b) empower the Governor-General to make regulations exempting state and territory incorporated bodies from coverage of the *Privacy Act* on public interest grounds.

Proposal 34–6 The *Privacy Act* should be amended to provide that, in considering whether to exempt state and territory incorporated bodies from coverage of the *Privacy Act*, the Minister must:

(a) be satisfied that the state or territory has requested that the body be exempt from the Act;

(b) consider:

(i) whether coverage of the body under the *Privacy Act* adversely affects the state or territory government;

(ii) the desirability of regulating under the *Privacy Act* the handling of personal information by that body; and

(iii) whether the state or territory law regulates the handling of personal information by that body to a standard that is at least equivalent to the standard that would otherwise apply to the body under the *Privacy Act*; and

(c) consult with the Privacy Commissioner about the matters mentioned in paragraphs (ii) and (iii) above.

35. Small Business Exemption

Proposal 35–1 The *Privacy Act* should be amended to remove the small business exemption by:

(a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and

(b) repealing ss 6D–6EA of the Act.

Proposal 35–2 Before the proposed removal of the small business exemption from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by:

(a) establishing a national small business hotline to assist small businesses in complying with the Act;

(b) developing educational materials—including guidelines, information sheets, fact sheets and checklists—on the requirements under the Act;

(c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge; and

(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding and acceptance of the privacy principles.

36. Employee Records Exemption

Proposal 36–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.

Proposal 36–2 The *Privacy Act* should be amended to provide that an agency or organisation may deny a request for access to evaluative material, disclosure of which would breach an obligation of confidence to the supplier of the information. 'Evaluative material' for these purposes means evaluative or opinion material compiled solely for the purpose of determining the suitability, eligibility, or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit.

37. Political Exemption

Proposal 37–1 The *Privacy Act* should be amended to remove the exemption for registered political parties and the exemption for political acts and practices by:

(a) deleting the reference to a 'registered political party' from the definition of 'organisation' in s 6C(1) of the Act;

(b) repealing s 7C of the Act; and

(c) removing the partial exemption that is currently applicable to Australian Government ministers in s 7(1) of the Act.

Proposal 37–2 The *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.

Proposal 37–3 Before the proposed removal of the exemptions for registered political parties and for political acts and practices from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act.

38. Media Exemption

Proposal 38–1 The *Privacy Act* should be amended to define 'journalism' to mean the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs or a documentary; or

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary.

Proposal 38–2 In consultation with the Australian Communications and Media Authority and peak media representative bodies, the Office of the Privacy Commissioner should establish criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

Proposal 38–3 The Office of the Privacy Commissioner should issue guidelines containing the criteria for assessing the adequacy of media privacy standards established under Proposal 38–2.

Proposal 38–4 Section 7B(4)(b)(i) of the *Privacy Act* should be amended to provide that the standards must 'deal *adequately* with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters)'.

Proposal 38–5 The Office of the Privacy Commissioner should issue guidance to clarify that the term 'publicly committed' in s 7B(4) of the *Privacy Act* requires both:

(a) express commitment by a media organisation to observe privacy standards that have been published in writing by the media organisation or a person or body representing a class of media organisations; and

(b) conduct by the media organisation evidencing commitment to observe those standards.

40. New Exemptions

Question 40–1 Should the Australian Government request that the Standing Committee of Attorneys-General consider the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry?

Question 40–2 Should the *Privacy Act* or other relevant legislation be amended to provide exemptions or exceptions applicable to the operation of alternative dispute resolution (ADR) schemes? Specifically, should the proposed:

(a) 'Specific Notification' principle exempt or except ADR bodies from the requirement to inform an individual about the fact of collection of personal information, including unsolicited personal information, where to do so would prejudice an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another individual;

(b) 'Use and Disclosure' principle authorise the disclosure of personal and sensitive information to ADR bodies for the purpose of dispute resolution; and

(c) 'Sensitive Information' principle authorise the collection of sensitive information without consent by an ADR body where necessary for the purpose of dispute resolution?

Part F—Office of the Privacy Commissioner

43. Structure of the Office of the Privacy Commissioner

Proposal 43–1 The *Privacy Act* should be amended to change the name of the 'Office of the Privacy Commissioner' to the 'Australian Privacy Commission'.

Proposal 43–2 Part IV, Division 1 of the *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioners may exercise all the powers, duties and functions of the Privacy Commissioner under this Act—including a power conferred by s 52 and a power in connection with the performance of the function of the Privacy Commissioner set out in s 28(1)(a)—or any other enactment.

Proposal 43–3 Section 29 of the *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act, as set out in Proposal 3–4, in the performance of his or her functions and the exercise of his or her powers.

Proposal 43–4 Section 82 of the *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee:

(a) require the appointment of a person to represent the health sector;

(b) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven; and

(c) replace 'electronic data-processing' in s 82(7)(c) with 'information and communication technologies'.

Proposal 43–5 The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion to advise the Privacy Commissioner.

44. Powers of the Office of the Privacy Commissioner

Proposal 44–1 The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c) of the *Privacy Act*.

Proposal 44–2 The *Privacy Act* should be amended to reflect that where guidelines issued by the Privacy Commissioner are binding they should be renamed 'rules'. For example, the following should be renamed to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*:

(a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed *Tax File Number Rules*;

(b) Medicare and Pharmaceutical Benefits Programs Privacy Guidelines (issued under s 135AA of the *National Health Act 1953* (Cth)) should be renamed the *Medicare and Pharmaceutical Benefits Programs Privacy Rules*;

(c) Data Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth)) should be renamed the *Data Matching Program (Assistance and Tax) Rules*; and

(d) Guidelines for National Privacy Principles about genetic information should be renamed *Genetic Information Privacy Rules*.

Proposal 44–3 Following the adoption of Proposal 21–1 to require agencies to produce and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.

Proposal 44–4 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and

(b) report to the Minister an agency or organisation's failure to comply with such a direction.

Proposal 44–5 The Office of the Privacy Commissioner should develop Privacy Impact Assessment Guidelines tailored to the needs of organisations.

Proposal 44–6 The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct audits of the records of personal information maintained by

organisations for the purpose of ascertaining whether the records are maintained according to the proposed Unified Privacy Principles (UPPs), Privacy Regulations, Rules and any privacy code that binds the organisation.

Proposal 44–7 The Office of the Privacy Commissioner should maintain and publish on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.

Proposal 44–8 The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a public interest determination where the Privacy Commissioner is satisfied that the application is frivolous, vexatious, misconceived or lacking in merit.

Proposal 44–9 Part IIIAA of the *Privacy Act* should be amended to specify that:

(a) privacy codes approved under Part IIIAA operate in addition to the proposed UPPs and do not replace those principles; and

(b) a privacy code may provide guidance or standards on how any one or more of the proposed UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that are at least equivalent to those under the Act.

Proposal 44–10 Part IIIAA of the *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) request the development of a privacy code to be approved by the Privacy Commissioner pursuant to s 18BB; and

(b) develop and impose a privacy code that applies to designated agencies and organisations.

45. Investigation and Resolution of Privacy Complaints

Proposal 45–1 Section 41(1) of the *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under s 36, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that:

(a) the complainant has withdrawn the complaint; or

(b) the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or

(c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.

Proposal 45–2 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) decline to investigate a complaint where the complaint is being handled by an approved external dispute resolution scheme; or

(b) decline to investigate a complaint that would be more suitably handled by an approved external dispute resolution scheme, and to refer that complaint to the external dispute resolution scheme with a request for investigation.

Proposal 45–3 Section 99 of the *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers, including a power conferred by section 52, in relation to complaint handling conferred on the Commissioner by the *Privacy Act*.

Proposal 45–4 Sections 27(1)(a) and (ab) of the *Privacy Act* should be amended to make it clear that the Privacy Commissioner's functions in relation to complaint handling include:

(a) to receive complaints about an act or practice that may be an interference with the privacy of an individual;

(b) to investigate the act or practice about which a complaint has been made; and

(c) where the Commissioner considers it appropriate to do so and at any stage after acceptance of the complaint, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint or to make a determination in respect of the complaint under s 52.

Proposal 45–5 The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following:

(a) If, at any stage after receiving the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make all reasonable attempts to conciliate the complaint.

(b) Where, in the opinion of the Commissioner, all reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that

conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

(c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.

Proposal 45–6 Section 52 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make an order in a determination that an agency or respondent must take specified action within a specified period for the purpose of ensuring compliance with the Act.

Proposal 45–7 The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner under s 52 and the current review rights set out in s 61 should be repealed.

Proposal 45–8 The Office of the Privacy Commissioner should prepare and publish a document setting out its complaint-handling policies and procedures.

Proposal 45–9 Section 38B(2) of the *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member has not consented to be a class member.

Proposal 45–10 Section 42 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make preliminary inquiries of third parties as well as the respondent.

Proposal 45–11 Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference.

Proposal 45–12 Section 69(1) and (2) of the *Privacy Act* should be deleted, which would allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.

Proposal 45–13 The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if:

(a) the Privacy Commissioner considers that the matter could be determined fairly on the basis of written submissions by the parties; and

(b) the complainant and respondent consent to the matter being determined without oral submissions.

46. Enforcing the *Privacy Act*

Proposal 46–1 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;

(b) prescribe in the notice that an agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*; and

(c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.

Proposal 46–2 The *Privacy Act* should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual. The Office of the Privacy Commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty is made.

47. Data Breach Notification

Proposal 47–1 The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:

(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

(b) An agency or organisation is not required to notify any affected individual where:

  (i) the specified information was encrypted adequately;

  (ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy

Principles (provided that the personal information is not used or subject to further unauthorised disclosure); or

(iii) the Privacy Commissioner does not consider that notification would be in the public interest.

(c) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

Part G—Credit Reporting Provisions

50. The Approach to Reform

Proposal 50–1 The credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and proposed Unified Privacy Principles (UPPs).

Proposal 50–2 Privacy rules, which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be promulgated in regulations under the *Privacy Act*—the proposed *Privacy (Credit Reporting Information) Regulations*.

Proposal 50–3 The obligations imposed on credit reporting agencies and credit providers by the proposed *Privacy (Credit Reporting Information) Regulations* should be in addition to those imposed by the proposed UPPs.

Proposal 50–4 The proposed *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the proposed UPPs.

Proposal 50–5 The proposed *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.

Proposal 50–6 The definition of a 'credit reporting business' in the proposed *Privacy (Credit Reporting Information) Regulations*, if based on that in s 6(1) of the *Privacy Act*, should exclude the phrase 'other than records in which the only personal information relating to individuals is publicly available information'.

Proposal 50–7 The proposed *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* (whether by operation of s 11B of the *Privacy Act* or pursuant

to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

Question 50–1 Should organisations be regarded as credit providers if they make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least thirty days as compared to seven days, as is currently the case under the OPC's *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)*?

Question 50–2 Should the definition of 'credit provider' under the *Credit Reporting Privacy Code* 2004 (NZ) be adopted as the definition of 'credit provider' under the proposed *Privacy (Credit Reporting Information) Regulations*? That is, should 'credit provider' be defined simply as 'a person that carries on a business involving the provision of credit to an individual'; and credit as 'property or services acquired before payment, and money on loan'?

Proposal 50–8 The proposed *Privacy (Credit Reporting Information) Regulations* should exclude: the reporting of personal information about foreign credit and foreign credit providers; and the disclosure of credit reporting information to foreign credit providers.

Proposal 50–9 The Australian Government should consider including credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).

Proposal 50–10 The proposed *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit advanced to an individual for any purpose and not limited to 'domestic, family or household' purposes as is currently the case under the definition of 'credit' in the *Privacy Act*.

Proposal 50–11 Credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, an industry code dealing with operational matters such as default reporting obligations and protocols and procedures for the auditing of credit reporting information.

51. More Comprehensive Credit Reporting

Proposal 51–1 The proposed *Privacy (Credit Reporting Information) Regulations* should permit the inclusion in credit reporting files of the following categories of personal information in addition to those currently permitted under s 18E of the *Privacy Act*:

(a) the type of each current credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each current credit account was opened;

(c) the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and

(d) the date on which each credit account was closed.

Proposal 51–2 The credit reporting industry code (see Proposal 50–11) should provide for access to information on credit information files according to principles of reciprocity. That is, in general, credit providers only should have access to the same categories of personal information that they provide to the credit reporting agency.

Proposal 51–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for a review after five years of operation. The review should focus on the impact of more comprehensive credit reporting on privacy and the credit market.

52. Collection of Credit Reporting Information

Proposal 52–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.

Proposal 52–2 Credit reporting agencies only should be permitted to list overdue payments of more than a minimum amount.

Question 52–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide a minimum amount for overdue payments listed by credit reporting agencies? If not, by what mechanism should a minimum amount for overdue payments be set and enforced?

Proposal 52–3 The proposed *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques, as currently permitted under s 18E(1)(b)(vii) of the *Privacy Act*.

Proposal 52–4 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index (NPII) administered under the *Bankruptcy Regulations 1966* (Cth).

Proposal 52–5 Credit reporting agencies, in accordance with obligations to ensure the accuracy and completeness of credit reporting information, should ensure that

credit reports adequately differentiate the forms of administration identified on the NPII.

Question 52–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow for the listing of a 'serious credit infringement' or similar and, if so, how should this concept be defined?

Proposal 52–6 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information.

Proposal 52–7 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as that term is defined in s 6(1) of the *Privacy Act*.

Proposal 52–8 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information about individuals the credit provider or credit reporting agency knows to be under the age of 18 years.

Proposal 52–9 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, at or before the time credit reporting information is collected about an individual, credit providers must take reasonable steps to ensure that the individual is aware of:

(a) the fact and circumstances of collection (for example, how and where the information was collected);

(b) the credit provider's and credit reporting agency's identity and contact details;

(c) the fact that the individual is able to gain access to the information;

(d) the main consequences of not providing the information;

(e) the types of people, organisations, agencies or other entities to whom the credit provider and credit reporting agency usually discloses credit reporting information; and

(f) the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her credit reporting information.

Proposal 52–10 The proposed *Privacy (Credit Reporting Information) Regulations* should prescribe the specific circumstances in which a credit provider must inform an individual that personal information might be disclosed to a credit reporting agency, for example, in circumstances where the individual defaults in making payments.

Question 52–3 In what specific circumstances should a credit provider be obliged to inform an individual that personal information might be disclosed to a credit reporting agency; and what information should notices contain? Who should give notice when a debt is assigned—the original credit provider, the assignee or both?

Question 52–4 Should the proposed *Privacy (Credit Reporting Information) Regulations* prescribe specific circumstances in which a credit reporting agency must inform an individual that it has collected personal information?

53. Use and Disclosure of Credit Reporting Information

Proposal 53–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information, based on those uses and disclosures currently permitted under ss 18K, 18L and 18N of the *Privacy Act*.

Proposal 53–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, in addition, a credit reporting agency or credit provider may use or disclose credit reporting information for related secondary purposes, as permitted by the proposed 'Use and Disclosure' principle.

Question 53–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow credit providers (but not credit reporting agencies) to disclose an individual's credit reporting information to a mortgage or trade insurer, where access to the information is required to assist in the assessment of the individual's credit worthiness?

Proposal 53–3 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing.

Question 53–2 Should credit providers be permitted to use credit reporting information to 'pre-screen' credit offers? If so, should credit providers be required to allow individuals to opt out, or should credit providers only be permitted to engage in pre-screening if the individual in question has expressly opted in to receiving credit offers?

Question 53–3 If the use and disclosure of credit reporting information for identity verification purposes is not authorised under the proposed *Privacy (Credit Reporting Information) Regulations*, what other sources of data might be used by credit providers to satisfy obligations under the *Anti-Money Laundering* and *Counter-Terrorism Financing Act 2006* (Cth) and similar legislation? What are the advantages and disadvantages of the alternate sources of data?

Proposal 53–4 There should be no equivalent in the proposed *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information related to credit worthiness. The use and disclosure limitations should apply only to personal information maintained by credit reporting agencies and used in credit reporting.

54. Data Quality and Security

Proposal 54–1 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a State or a Territory from bringing proceedings against the individual to recover the amount of the overdue payment.

Proposal 54–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt, such as by entering into a scheme of arrangement with the credit provider, an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information file for the full five year period permissible under the regulations.

Proposal 54–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure data quality in the information credit providers provide to credit reporting agencies;

(b) establish and maintain controls to ensure that only information that is accurate, complete, up-to-date and relevant is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

Proposal 54–4 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that credit reporting information is accurate, up-to-date, complete and not misleading.

Proposal 54–5 The credit reporting industry code (see Proposal 50–11) should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers. These procedures should deal with matters including:

(a) the timeliness of the reporting of personal information, such as overdue payments;

(b) the calculation of overdue payments for credit reporting purposes;

(c) obligations to prevent the multiple listing of the same debt;

(d) the updating of personal information reported, including where schemes of arrangement have been entered into; and

(e) the linking of credit reporting information where it is unclear whether the information relates to more than one individual with similar identifying details or to one individual who has used different identifying details.

Proposal 54–6 The proposed review of the *Privacy (Credit Reporting Information) Regulations* after five years' of operation (Proposal 51–3) also should consider whether further regulation is required to ensure the data quality of credit reporting information.

Proposal 54–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

Proposal 54–8 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of information about voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

Proposal 54–9 The proposed *Privacy (Credit Reporting Information) Regulations* should contain no equivalent to s 18G(b) and (c), dealing with the security of credit information files and credit reports, as these obligations are adequately covered by the proposed 'Data Security' principle.

55. Rights of Access, Complaint Handling and Penalties

Question 55–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide that individuals have the right to obtain a free copy of their credit reporting information?

Question 55–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide an equivalent to s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised by a person authorised in writing and for a credit-related purpose?

Proposal 55–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to access and correct credit reporting information based on the provisions currently set out in ss 18H and 18J of the *Privacy Act*.

Proposal 55–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to be notified where a credit provider refuses an application for credit based wholly or partly on credit reporting information, based on the provisions currently set out in s 18M of the *Privacy Act*.

Proposal 55–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed.

Proposal 55–4 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that:

(a) credit reporting agencies and credit providers must handle credit reporting complaints in a fair, efficient and timely manner;

(b) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint;

(c) a credit reporting agency should refer to a credit provider for resolution of a complaint about the content of credit reporting information provided to the agency by that credit provider; and

(d) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint it must immediately inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

Proposal 55–5 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

Proposal 55–6 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where

the credit provider is a member of an external dispute resolution scheme approved by the Office of the Privacy Commissioner.

Proposal 55–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers have an obligation to provide evidence to individuals and dispute resolution bodies to substantiate disputed credit reporting information, such as default listings, and that if the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned.

Proposal 55–8 The *Privacy Act* should be amended to:

(a) remove the credit reporting offences by repealing ss 18C(4), 18D(4), 18K(4), 18L(2), 18N(2), 18R(2), 18S(3) and 18T; and

(b) allow a civil penalty to be imposed where there is a serious or repeated breach of the proposed *Privacy (Credit Reporting Information) Regulations*.

Part H—Health Services and Research

56. Regulatory Framework for Health Information

Proposal 56–1 The Privacy Commissioner should consider delegating the power to handle complaints under the *Privacy Act* in relation to interferences with health information privacy by organisations to state and territory health complaint agencies.

Proposal 56–2 Health information should continue to be regulated under the general provisions of the *Privacy Act* and the proposed Unified Privacy Principles (UPPs). Amendments to the proposed UPPs that relate specifically to the handling of health information should be promulgated in regulations under the *Privacy Act*—the *Privacy (Health Information) Regulations*.

Proposal 56–3 The Office of the Privacy Commissioner should publish a document bringing together the proposed UPPs and the amendments set out in the *Privacy (Health Information) Regulations*. This document will contain a complete set of the proposed UPPs as they relate to health information.

Proposal 56–4 The Office of the Privacy Commissioner—in consultation with the Australian Government Department of Health and Ageing and other relevant stakeholders—should develop guidelines on the handling of health information under the *Privacy Act* and the *Privacy (Health Information) Regulations*.

Proposal 56–5 The national Unique Healthcare Identifiers (UHIs) scheme and the national Shared Electronic Health Records (SEHR) scheme should be established

under specific enabling legislation. The legislation should address information privacy issues, such as:

(a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

(b) the eligibility criteria, rights and requirements for participation in the UHI scheme and the SEHR scheme by health consumers and health service providers, including consent requirements;

(c) permitted and prohibited uses and linkages of the personal information held in the systems;

(d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and

(e) safeguards in relation to the use of UHIs; for example, that it is not necessary to use a UHI in order to access health services.

57. The Privacy Act and Health Information

Proposal 57–1 The definition of 'health information' in the *Privacy Act* should be amended to make express reference to information or an opinion about the *physical*, *mental or psychological* health or disability of an individual.

Proposal 57–2 The *Privacy Act* should be amended to define a 'health service' as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, record, maintain or improve the individual's health;

  (ii) diagnose the individual's illness, injury or disability; or

  (iii) treat the individual's illness, injury or disability or suspected illness, injury or disability; or

(b) a disability service, palliative care service or aged care service; or

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Proposal 57–3 The *Privacy (Health Information) Regulations* should provide that a health service provider may collect health information from a health consumer, or a person responsible for the health consumer, about third parties without consent when:

(a) the collection of the third party's information into a health consumer's social, family or medical history is necessary to enable health service providers to provide a health service directly to the consumer; and

(b) the third party's information is relevant to the family, social or medical history of that consumer.

Question 57–1 Should the proposed *Privacy (Health Information) Regulations* provide that health information may be collected without consent where it is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose?

Proposal 57–4 The provisions of National Privacy Principle 2 dealing with the disclosure of health information in the health services context to a person responsible for an individual should be moved to the *Privacy (Health Information) Regulations*. The proposed regulation should:

(a) be expressed to apply to both agencies and organisations;

(b) provide that an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if the individual is 'incapable of giving consent' to the disclosure and all the other circumstances currently set out in NPP 2.4 are met;

(c) include a definition of a person 'responsible' for an individual amended to incorporate the term 'authorised representive'; and

(d) refer to 'de facto partner' rather than 'de facto spouse'.

Proposal 57–5 National Privacy Principle 2.1(ea) on the use and disclosure of genetic information should be moved to the *Privacy (Health Information) Regulations* and amended to apply to both agencies and organisations. Any use or disclosure under the proposed regulation should be in accordance with binding rules issued by the Privacy Commissioner.

Proposal 57–6 The *Privacy (Health Information) Regulations* should provide that, if an organisation denies an individual access to his or her own health information on the ground that providing access would be reasonably likely to pose a serious threat to the life or health of any individual, the:

(a) organisation must advise the individual that he or she may nominate a registered medical practitioner to be given access to the health information;

(b) individual may nominate a registered medical practitioner and request that the organisation provide access to the information to the nominated medical practitioner;

(c) organisation must provide access to the health information to the nominated medical practitioner; and

(d) nominated medical practitioner may assess the grounds for denying access to the health information and may provide the individual with sufficient access to the information to meet the individual's needs if he or she is satisfied that to do so would not be likely to pose a serious threat to the life or health of any individual.

Proposal 57–7 The *Privacy (Health Information) Regulations* should provide that where a health service practice or business is sold, amalgamated or closed down and a health service provider will not be providing health services in the new practice or business, or the provider dies, the provider, or the legal representative of the provider, must take all reasonable and appropriate steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service or the death of the health service provider; and

(b) inform them about proposed arrangements for the transfer or storage of individuals' health information.

Proposal 57–8 The *Privacy (Health Information) Regulations* should provide that if an individual:

(a) requests that a health service provider, or the health service provider's legal representative, make the individual's health information available to another health service provider; or

(b) authorises a health service provider to request that another health service provider transfers the individual's health information to the requesting health service provider,

the health service provider must transfer the individual's health information as requested. The health information may be provided in summary form.

Proposal 57–9 The *Privacy (Health Information) Regulations* should make express provision for the collection, use and disclosure of health information without

consent where necessary for the funding, management, planning, monitoring, improvement or evaluation of a health service where:

(a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual;

(b) it is impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

(c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

Proposal 57–10 The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, improvement or evaluation of a health service.

58. Research

Proposal 58–1 The Privacy Commissioner should issue one set of rules under the proposed exceptions to the 'Collection' principle and the 'Use and Disclosure' principle in the Unified Privacy Principles (UPPs) to replace the *Guidelines Under Section 95 of the Privacy Act 1988* and the *Guidelines Approved Under Section 95A of the Privacy Act 1988*.

Proposal 58–2 The *Privacy Act* should be amended to extend the existing arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

Proposal 58–3 The *Privacy Act* should be amended to provide that 'research' is any activity, including the compilation or analysis of statistics, subject to review by a Human Research Ethics Committee under the *National Statement on Ethical Conduct in Human Research* (2007).

Proposal 58–4 The research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle should provide that before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.

Proposal 58–5 The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, to ensure that the approaches adopted in the rules and the *National Statement on Ethical Conduct in Human Research* (2007) are compatible.

Proposal 58–6 The *National Statement on Ethical Conduct in Human Research* (2007) should be amended to require that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act,* it must be reviewed and approved by a Human Research Ethics Committee.

Proposal 58–7 In developing the rules to be issued in relation to research under the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, the Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements currently imposed on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

Proposal 58–8 The research exception to the proposed 'Collection' principle should state that, despite subclause 2.6, an agency or organisation may collect sensitive information about an individual where:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

(e) the information is collected in accordance with rules issued by the Privacy Commissioner.

Where an agency or organisation collects sensitive information about an individual in accordance with this provision, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Proposal 58–9 The research exception to the proposed 'Use and Disclosure' principle should state that despite the other provisions of the Use and Disclosure principle, an agency or organisation may use or disclose personal information where:

(a) the use or disclosure is necessary for research;

(b) it is impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

(c) a Human Research Ethics Committee has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs;

(d) the information is used or disclosed in accordance with rules issued by the Privacy Commissioner; and

(e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the personal information in a form that would identify the individual or from which the individual would be reasonably identifiable.

Proposal 58–10 The Privacy Commissioner should provide guidance on the meaning of 'not reasonably identifiable'.

Proposal 58–11 The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:

(a) the process by which a Human Research Ethics Committee should review a proposal to establish a health information database or register for research purposes;

(b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in establishing the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

(c) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

Proposal 58–12 The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:

(a) the process by which a Human Research Ethics Committee should review a proposal to examine a health information database or register to identify potential participants in research; and

(b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in allowing the examination of the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the UPPs.

Proposal 58–13 Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should consult the Office of the Privacy Commissioner to ensure that the systems or infrastructure they are developing meet the requirements of the *Privacy Act*.

Part I—Children, Young People and Adults Requiring Assistance

59. Children, Young People and Privacy

Proposal 59–1 The Australian Government should fund a longitudinal study of the attitudes of Australians, including young Australians, to privacy.

Proposal 59–2 The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.

Proposal 59–3 NetAlert should include specific guidance on using social networking sites as part of its educational material on internet safety.

Proposal 59–4 In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curricula.

60. Decision Making by People Under the Age of 18

Proposal 60–1 The *Privacy Act* should be amended to provide that:

(a) an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable (in accordance with the criteria set out in Proposal 60–2) of giving that consent, making that request or exercising that right;

(b) where it is practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, an assessment about the individual's capacity should be undertaken; and

(c) where it is not practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, then the consent, request or exercising of the right to access must be provided by an authorised representative of the individual.

Proposal 60–2 The *Privacy Act* should be amended to provide that an individual aged under 18 is incapable of giving consent, making a request or exercising a right if, despite the provision of reasonable assistance by another person, he or she is incapable, by reason of maturity, injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

(b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.

Where an individual under the age of 18 is considered incapable of giving consent, making a request or exercising a right, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of that individual.

Proposal 60–3 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and their authorised representatives in decision-making processes;

(b) situations where children and young people are capable of giving consent, making a request or exercising a right on their own behalf;

(c) practices and criteria to be used in determining whether a child or young person is incapable of giving consent, making a request or exercising a right on his or her own behalf;

(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and

(e) the requirements to obtain consent from an authorised representative of a child or young person in appropriate circumstances.

Proposal 60–4 The *Privacy Act* should be amended to provide that an agency or organisation will not be considered to have acted without consent if it did not know, and could not reasonably be expected to have known from the information available, that an individual was aged 14 or under, and the agency or organisation acted upon the consent given by the individual.

Proposal 60–5 An agency or organisation that handles the personal information of individuals under the age of 18 should address in its Privacy Policy how such information is managed.

Proposal 60–6 An agency or organisation that regularly handles the personal information of individuals under the age of 18 should ensure that its staff are adequately trained to assess the decision-making capacity of children and young people.

Proposal 60–7 Schools should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:

(a) will be disclosed to, or withheld from, persons with parental responsibility; and

(b) collected by school counsellors will be disclosed to the school management, persons with parental responsibility, or others.

Proposal 60–8 The Office of the Privacy Commissioner should include consideration of the privacy of children and young people in the proposed criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

61. Adults with a Temporary or Permanent Incapacity

Question 61–1 Should the *Privacy Act* be amended to provide expressly that all individuals aged 18 and over are presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable of giving that consent, making that request or exercising that right?

Proposal 61–1 The *Privacy Act* should be amended to provide that an individual aged 18 or over is incapable of giving consent, making a request or exercising a right under the Act if, despite the provision of reasonable assistance by another person, he or she is incapable by reason of injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability, or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

(b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.

Where an individual is considered incapable of giving consent, making a request or exercising a right under the Act, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of the individual.

Proposal 61–2 The *Privacy Act* should be amended to introduce the concept of 'authorised representative', defined as a person who is, in relation to an individual:

(a) a guardian of the individual appointed under law;

(b) a guardian for the individual under an appointment of enduring guardianship;

(c) an attorney for the individual under an enduring power of attorney;

(d) a person who has parental responsibility for the individual if the individual is under the age of 18; or

(e) otherwise empowered under law to perform any functions or duties as agent or in the best interests of the individual.

The *Privacy Act* should state that an authorised representative is not to act on behalf of the individual in any way that is inconsistent with an order made by a court or tribunal, in contravention of the terms of any appointment under law, or beyond the powers provided for in an enduring power of attorney.

Question 61–2 Should the definition of 'authorised representative' include a person who was nominated by the individual at a time when the individual had the capacity to make the nomination?

Proposal 61–3 The *Privacy Act* should be amended to provide that an agency or organisation that has taken reasonable steps to validate the authority of an authorised representative will not be considered to have engaged in conduct constituting an interference with privacy of an individual merely because it acted upon the consent, request or exercise of a right by that authorised representative, if it is later found that the authorised representative:

(a) was not properly appointed; or

(b) exceeded the authority of his or her appointment.

Proposal 61–4 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals aged 18 and over

incapable of giving consent, making a request or exercising a right on their own behalf, including on:

(a) the provision of reasonable assistance to individuals to understand and communicate decisions; and

(b) practices and criteria to be used in determining whether an individual is incapable of giving consent, making a request or exercising a right on his or her own behalf.

Proposal 61–5 Agencies and organisations that handle personal information about people incapable of making a decision should address in their Privacy Policies how such information is managed.

Proposal 61–6 Agencies and organisations that regularly handle personal information about adults incapable of making a decision should ensure that their staff are trained adequately to assess the decision-making capacity of individuals.

62. Other Third Party Assistance

Proposal 62–1 Practice and procedures allowing for the involvement of third parties to assist an individual to make and communicate privacy decisions should be developed and published in guidance issued by the Office of the Privacy Commissioner.

Question 62–1 Should the *Privacy Act* be amended expressly to allow a third party nominated by the individual to give consent, make a request or exercise a right of access on behalf of the individual, either for one-off or long term arrangements?

Part J—Telecommunications

63. *Telecommunications Act*

Proposal 63–1 The Australian Government should initiate a review to consider the extent to which the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how the Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation; and

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Australian Government Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance.

Question 63–1 Sections 279 and 296 of the *Telecommunications Act 1997* (Cth) permit the use or disclosure by a person of information or a document if the use or disclosure is made 'in the performance of the person's duties' as an employee or contractor. Is the exception too broadly drafted? Is it resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined?

Proposal 63–2 Sections 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the proposed 'Use and Disclosure' principle under the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

Question 63–2 Does the Telecommunications (Interception and Access) Amendment Bill 2007 provide adequate protection of personal information that is used or disclosed for law enforcement purposes? For example, should the Bill be amended to:

(a) define 'telecommunications data';

(b) provide greater guidance on how the privacy implications of an authorisation should be considered and documented under proposed s 180(5);

(c) include positive obligations on law enforcement agencies to destroy in a timely manner irrelevant material containing personal information and information which is no longer needed; and

(d) provide that the Inspector-General of Intelligence and Security monitor the use of powers by the Australian Security Intelligence Organisation to obtain prospective telecommunications data?

Proposal 63–3 Sections 287 and 300 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a person of information or a document is permitted if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

  (i) a person's life, health or safety; or

  (ii) public health or public safety.

Proposal 63–4 Section 289 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(a) the other person has consented to the use or disclosure; or

(b) if the use or disclosure is for a purpose other than the primary purpose for which the information was collected (the secondary purpose):

  (i) the secondary purpose is related to the primary purpose and, if the information or document is sensitive information (within the meaning of the *Privacy Act 1988* (Cth)), the secondary purpose is directly related to the primary purpose of collection; and

  (ii) the other person would reasonably expect the person to use or disclose the information.

Proposal 63–5 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that 'consent' means 'express or implied consent'.

Question 63–3 How does s 290 of the *Telecommunications Act 1997* (Cth) operate in practice? Is the exception resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined?

Question 63–4 Is the exception that permits the use or disclosure of information or a document for certain business needs of other carriers or service providers (s 291 and s 302 of the *Telecommunications Act 1997* (Cth)) resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined?

Should the exception be amended to provide that silent and other blocked calling numbers can only be used or disclosed with a person's consent?

Proposal 63–6 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that use or disclosure by a person credit reporting information is to be handled in accordance with the *Privacy Act*.

Proposal 63–7 The Australian Government should amend the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* to provide that the test of research in the public interest is met when the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.

Proposal 63–8 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Office of the Privacy Commissioner, as soon as practicable after becoming aware:

(a) of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information; and

(b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.

Question 63–5 Should directory products that are produced from data sources other than the Integrated Public Number Database be subject to the same rules under Part 13 of the *Telecommunications Act 1997* (Cth) as directory products which are produced from data sourced from the Integrated Public Number Database?

Proposal 63–9 The *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

Proposal 63–10 Before the proposed removal of the small business exemption from the *Privacy Act* comes into effect (Proposal 35–1), the Australian Government should make regulations under s 6E of the *Privacy Act* to ensure that the Act applies to all small businesses in the telecommunications industry, including internet service providers and public number directory producers.

Question 63–6 Should a breach of Divisions 2, 4 and 5 of Part 13 of the *Telecommunications Act 1997* (Cth) attract a civil penalty rather than a criminal penalty?

Proposal 63–11 The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance and the Telecommunications Industry Ombudsman, should develop and publish guidance that addresses issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.

Proposal 63–12 Section 117(1)(k) of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority can only register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the code.

Proposal 63–13 Section 134 of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority only can determine, vary or revoke an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the standard.

Proposal 63–14 Section 306 of the *Telecommunications Act 1997* (Cth) should be amended to provide that each exception upon which a decision to disclose information or a document is based is to be recorded when that decision is based on more than one of the exceptions in Divisions 3 or 4 of Part 13 of the Act.

Proposal 63–15 Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

64. Other Telecommunications Privacy Issues

Question 64–1 Should ss 63B(1) and 135(3) of the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to clarify when an employee of a carrier may communicate or make use of lawfully intercepted or accessed information in the performance of his or her duties?

Question 64–2 How should the provisions that permit an employee of a carrier to communicate to another carrier intercepted or accessed information (ss 63B(2) and 135(4) of the *Telecommunications (Interception and Access) Act*) be clarified?

Question 64–3 Should further restrictions apply in relation to the use and disclosure of information obtained by a B-party interception warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth)?

Proposal 64–1 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

Proposal 64–2 The Attorney-General's Department should provide guidance on when the chief officer of an agency must cause information or a record to be destroyed when it is no longer required for a permitted purpose under s 79 and s 150 of the *Telecommunications (Interception and Access) Act 1979* (Cth). This guidance should include time limits within which agencies must review holdings of information and destroy information as required by the legislation.

Proposal 64–3 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to expressly require the destruction of non-material content intercepted under a B-party warrant.

Question 64–4 Should the regime relating to access to stored communications under the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to provide further reporting requirements in relation to the use and effectiveness of stored communications warrants?

Question 64–5 Should the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to provide for the role of a public interest monitor? If so, what should be the role of the monitor? Should its role include, for example, to:

(a) appear at any application made by an agency for interception and access warrants under the *Telecommunications (Interception and Access) Act*;

(b) test the validity of warrant applications;

(c) gather statistical information about the use and effectiveness of warrants;

(d) monitor the retention or destruction of information obtained under a warrant;

(e) provide to the Inspector General of Intelligence and Security, or other authority as appropriate, a report on non-compliance with the *Telecommunications (Interception and Access) Act*; or

(f) report to the Australian Parliament on the use of interception and access warrants?

Proposal 64–4 The Office of the Privacy Commissioner should be made a member of the Australian Communications and Media Authority's Law Enforcement Advisory Committee.

Question 64–6 Should the *Spam Act 2003* (Cth) be amended to:

(a) provide that the definition of 'electronic message' under s 5 includes Bluetooth messages;

(b) provide that facsimile messages are regulated under the Act;

(c) provide that an electronic message is required to include an unsubscribe message if the electronic message:

  (i) consists of no more than factual information; or

  (ii) has been authorised by a government body, a registered political party, a religious organisation, or a charity or charitable institution, and relates to goods or services; or

  (iii) has been authorised by an educational institution, and relates to goods or services;

(d) remove the exception for registered political parties?

Question 64–7 Should the *Do Not Call Register Act 2006* (Cth) be amended to remove the exception for registered political parties, independent members of parliament and candidates in an election?

Proposal 64–5 The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memoranda of understanding, addressing:

(a) the roles and functions of each of the bodies under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Privacy Act*;

(b) the exchange of relevant information and expertise between the bodies; and

(c) when a matter should be referred to, or received from, the bodies.

Proposal 64–6 The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Proposal 45–8), and its enforcement guidelines (see Proposal 46–2) should address:

(a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications

and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Privacy Act*; and

(b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.

Proposal 64–7 The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, Australian Communications Alliance and the Telecommunications Industry Ombudsman, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

(a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth);

(b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and

(c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

Proposal 64–8 The Office of the Privacy Commissioner, in consultation with the Attorney-General's Department, the Australian Communications and Media Authority, the Office of the Commonwealth Ombudsman, the Inspector General of Intelligence and Security and the Telecommunications Industry Ombudsman, should develop and publish educational material that addresses the:

(a) rules regulating privacy in the telecommunications industry;

(b) various bodies that are able to deal with a complaint in relation to privacy in the telecommunications industry, and how to make a complaint to those bodies.

Proposed Unified Privacy Principles (UPPs)

Contents

UPP 1.	Anonymity and Pseudonymity	89
UPP 2.	Collection	89
UPP 3.	Specific Notification	90
UPP 4.	Openness	91
UPP 5.	Use and Disclosure	92
UPP 6.	Direct Marketing (only applicable to organisations)	93
UPP 7.	Data Quality	94
UPP 8.	Data Security	94
UPP 9.	Access and Correction (only applicable to organisations)	95
UPP 10.	Identifiers	97
UPP 11.	Transborder Data Flows	98

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable, individuals, when transacting with an agency or organisation, should have the clear option of either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym, provided this would not be misleading.

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation collects personal information about an individual from the individual or from someone else, it must comply with UPP 3.

2.5 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

(a) destroy the information immediately without using or disclosing it; or

(b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.6 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required or specifically authorised by or under law; or

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent; or

(d) if the information is collected in the course of the activities of a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

UPP 3. Specific Notification

3.1 At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

(a) fact and circumstances of collection (for example, how, when and from where the information was collected);

(b) identity and contact details of the agency or organisation;

(c) fact that the individual is able to gain access to the information;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and

(g) avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

3.2 Where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of:

(a) the matters listed in UPP 3.1 above; and

(b) the source of the information, if requested by the individual.

3.3 An agency or organisation must comply with the obligations in UPPs 3.1 and 3.2:

(a) in circumstances where a reasonable person would expect to be notified; and

(b) except to the extent that:

(i) making the individual aware of these matters would pose a serious threat to the life or health of any individual;

(ii) in the case of an agency, the agency is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out the agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation in question;

(e) the types of individual about whom records are kept;

(f) the period for which each type of record is kept; and

(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically, for example, on its website (if it possesses one); and

(b) in hard copy, on request.

UPP 5. Use and Disclosure

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

(i) an individual's life, health or safety; or

(ii) public health or public safety; or

(d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(e) the use or disclosure is required or authorised by or under law; or

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

5.2 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note: Agencies and organisations are also subject to the requirements of the 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

UPP 6. Direct Marketing (only applicable to organisations)

6.1 An organisation must not use or disclose personal information about an individual for the primary purpose or a secondary purpose of direct marketing unless all of the following conditions are met:

(a) the individual has consented, or both of the following apply:

(i) the information is not sensitive information; and

(ii) it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and

(b) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(c) the individual has not made a request to the organisation not to receive direct marketing communications, and the individual has not withdrawn any consent he or she may have provided to the organisation to receive direct marketing communications;

(d) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(e) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be contacted directly electronically.

6.2 In the event that an individual makes a request of the organisation not to receive any further direct marketing communications, the organisation must comply with this requirement within a reasonable period of time.

6.3 An organisation must take reasonable steps, when requested by an individual to whom it has sent direct marketing communications, to advise the individual from where it acquired the individual's personal information.

UPP 7. Data Quality

An agency or organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the UPPs, accurate, complete, up-to-date and relevant.

UPP 8. Data Security

An agency or organisation must take reasonable steps to:

(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;

(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and

(c) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

UPP 9. Access and Correction (only applicable to organisations)

9.1 If an organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:

(a) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;

(b) providing access would have an unreasonable impact upon the privacy of other individuals;

(c) the request for access is frivolous or vexatious;

(d) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(f) providing access would be unlawful;

(g) denying access is required or authorised by or under law;

(h) providing access would be likely to prejudice an investigation of possible unlawful activity;

(i) providing access would be likely to prejudice the:

(i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) protection of the public revenue; or

(iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(j) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches UPP 9.1 if it relies on UPP 9.2 to give an individual an explanation for a commercially sensitive decision in circumstances where UPP 9.2 does not apply.

9.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs UPP 9.1(a) to (j) (inclusive), the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties.

9.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

9.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, the organisation must take reasonable steps to:

(a) correct the information so that it is accurate, complete, up-to-date and relevant; and

(b) notify any other entities to whom the personal information has already been disclosed prior to correction, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.6 If the individual and the organisation disagree about whether the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete, up-to-date or relevant, the organisation must take reasonable steps to do so.

9.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

Note: If an individual wishes to access, or have corrected, personal information that is held by an agency, the individual should follow the requirements set out in the relevant Part of this Act.

UPP 10. Identifiers

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.2 An agency must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) another agency;

(b) an agent of another agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.3 The requirements in NPPs 10.1 and 10.2 do not apply to the adoption by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2), as proposed to be amended.

10.4 Where an identifier has been 'assigned' within the meaning of UPP 10.1 or 10.2, an agency or organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the agency or organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure;

(c) the identifier is genetic information and the use or disclosure would be permitted by the proposed Privacy (Health Information) Regulations; or

(d) the use or disclosure is by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

10.5 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or any other particular that:

(a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or

(b) is determined to be an identifier by the Office of the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999*, is not an 'identifier'.

Note: A determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* (Cth).

UPP 11. Transborder Data Flows

An agency or organisation in Australia or an external Territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia only if:

(a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the UPPs; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

(vi) extradition and mutual assistance; or

(d) the agency of organisation continues to be liable for any breaches of the UPPs, and

(i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;

(ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

(iv) all of the following apply: the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

(v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the UPPs.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

1. Introduction to the Inquiry

Contents

Introduction 103
Key proposals for reform 105
Background 107
Privacy Act 110
The scope of the Inquiry 111
Terms of Reference 111
Related privacy references 112
VLRC privacy reference 112
NSWLRC privacy reference 113
NZLC privacy reference 114
Defining 'privacy' 114
Towards a working definition 118
Privacy beyond the individual 122
Background 122
Indigenous and other ethnic groups 124
Corporations and commercial entities 126
Submissions and consultations 127
ALRC's view 131
Organisation of this paper 136
Process of reform 140
Advisory Committee and Sub-committees 140
Community consultation and participation 140
Timeframe for the Inquiry 142

Introduction

1.1 On 30 January 2006, the Attorney-General, the Hon Philip Ruddock MP, asked the Australian Law Reform Commission (ALRC) to conduct an inquiry into the extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia.[1] To date in this Inquiry, the ALRC has published two issues papers, *Review of Privacy* (IP 31)[2] and *Review of*

1 Such a review was recommended in two previous inquiries: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 2; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 1.

2 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).

Privacy—Credit Reporting Provisions (IP 32).[3] To facilitate community involvement in the Inquiry, the ALRC also published a concise overview of IP 31 and IP 32, entitled *Reviewing Australia's Privacy Law—Is Privacy Passé?*[4]

1.2 The *Privacy Act* itself was substantially the product of a seven year research effort by the ALRC, which culminated in 1983 with the three volume report, *Privacy* (ALRC 22).[5] The Act also gave effect to Australia's obligations to implement the Organisation for Economic Co-operation and Development *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines),[6] and partially implemented into domestic law Australia's obligations under art 17 of the *International Covenant on Civil and Political Rights* (ICCPR).[7]

1.3 ALRC 22 was not the first report of the ALRC to consider the concept of privacy. One earlier report—*Unfair Publication: Defamation and Privacy* (ALRC 11)[8]—is worthy of particular note. In addition to making recommendations for reform in the law of defamation, ALRC 11 proposed some limited privacy protection. It was recommended that a person be allowed to sue for damages or an injunction

> if 'sensitive private facts', relating to health, private behaviour, home life, and personal or family relationships, were published about him which were likely in all the circumstances to cause distress, annoyance or embarrassment to a person in the position of the individual. Wide defences were proposed allowing publication of personal information if the publication was relevant to the topic of public interest.[9]

1.4 Since the enactment of the *Privacy Act*, advances in information, communication and surveillance technologies have created a range of previously unforeseen privacy issues. At the same time, the emergence of regional political and economic blocs, such as the European Union and Asia-Pacific Economic Cooperation group (APEC), has created pressure for the alignment of our privacy protection regime with those of our key trading partners. These issues are being considered in detail during the course of the Inquiry.

---

3 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006).

4 Australian Law Reform Commission, *Reviewing Australia's Privacy Laws—Is Privacy Passé?* (2006).

5 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed below, and in detail in Part D.

7 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.54]. Article 17 of the ICCPR provides: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks': *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

8 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).

9 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [6]. See generally Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [250]. How far Australia has progressed in recognising a common law right to privacy since the publication of ALRC 11 is discussed below.

Key proposals for reform

1.5 The current Inquiry is the one of the largest projects ever undertaken by the ALRC. In the three volumes of this Discussion Paper, approximately 300 proposals for reform are put forward for consideration. Some of the key proposals include the following:

- **Redrafting the Privacy Act and Privacy Principles.** The *Privacy Act* should be substantially redrafted to achieve greater logical consistency, simplicity and clarity. Such an amendment to the Act would include the unification of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) into a single set of privacy principles covering information handling in both the public and private sectors. For the purposes of this Inquiry, these principles are referred to as the Unified Privacy Principles (UPPs). This also would result in a restructuring of the Act to provide for high level principles of general application, regulations to address specific types of information, such as health and credit reporting information, and guidance issued by relevant regulators, such as the Privacy Commissioner.

- **Ensuring National Consistency.** Privacy laws should be much more consistent across all Australian jurisdictions. To achieve greater consistency, the *Privacy Act* should apply to the federal public sector and the private sector—to the exclusion of state and territory laws dealing specifically with the privacy of personal information, including personal health information, handled by organisations. Any state and territory privacy laws regulating the state or territory public sector should apply the proposed UPPs, and contain uniform provisions relating to a number of key issues—such as definitions, the making of determinations by the regulator, and data breach notification.

- **Updating Key Definitions.** Important definitions in the *Privacy Act*—such as the definition of 'personal information', 'sensitive information' and 'record'—should be updated to deal with new technologies and new methods of collecting and storing personal information.

- **Reduced Number of Exemptions.** The number of exemptions in the *Privacy Act* should be reduced. In particular, it is proposed that the Act be amended to remove the exemptions for small business, employee records and registered political parties. It must be noted, however, that the proposal to remove the small business exemption is predicated on the provision by the Office of the Privacy Commissioner (OPC) of support to small businesses to assist them in understanding and fulfilling their obligations under the *Privacy Act*, so as not to increase the regulatory burden to any significant degree.

- **Restructuring the OPC.** The OPC should be restructured. The name of the OPC should be changed to the Australian Privacy Commission, and the *Privacy Act* should be amended to increase the powers of the Privacy Commissioner. For example, it is proposed that the Privacy Commissioner should have the power to direct an agency or organisation to carry out a privacy impact assessment on a new project or development that may have a significant impact on the handling of personal information, and to conduct privacy audits of organisations.

- **Streamline Complaint Handling.** Complaint handling procedures should be streamlined. It is proposed that the Privacy Commissioner have the power to decline to investigate a complaint if, for example, the complaint is being handled by an appropriate external dispute resolution scheme.[10] Further, both complainants and respondents should have the power to require that the complaint be resolved by determination if, in the opinion of the Privacy Commissioner, all reasonable attempts to settle the complaint have failed.

- **Data Breach Notification.** The *Privacy Act* should be amended to include data breach notification provisions whereby an organisation or agency must notify the Privacy Commissioner and any affected individuals when a data breach has occurred which may give rise to serious harm to affected individuals.

- **Reform of the Credit Reporting Provisions.** The credit reporting provisions of the *Privacy Act* (Part IIIA) should be repealed and credit reporting regulated under the general provisions of the Act (including proposed credit reporting regulations), and the proposed UPPs. Further, there should be some expansion of the categories of personal information that can be included in credit reporting information held by credit reporting agencies, to include the: type of each current credit account opened; date on which each current credit account was opened; limit of each current credit account; date on which each credit account was closed. Credit providers should be prohibited from using or disclosing credit reporting information for the purposes of direct marketing, and may only list overdue payment information where the credit provider is a member of an external dispute resolution scheme approved by the OPC.

- **Presumption of Capacity.** The ALRC supports the individual assessment of the capacity of a child or young person to make decisions under the *Privacy Act*, but acknowledges it is not always practicable to conduct such assessments. The *Privacy Act* should be amended to provide that an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right

---

10 The term 'external dispute resolution' (EDR) is used in this Discussion Paper to refer to the resolution of complaints or disputes by an entity (other than a court, tribunal or government regulator) that is external to the organisation subject to the complaint or dispute. The term includes, but is not limited to, EDR conducted by EDR schemes approved by the Australian Securities and Investments Commission: see, *Corporations Act 2001* (Cth) ss 912A(2)(b), 1017G(2)(b).

of access concerning the individual's personal information, unless found to be incapable, on the basis of proposed criteria, of giving consent, making that request or exercising that right.

- **Reform of Part 13 of the *Telecommunications Act*** – Part 13 of the *Telecommunications Act 1997* (Cth), which deals with the use and disclosure of personal information in the telecommunications industry, should be redrafted to achieve greater logical consistency, simplicity and clarity. Further, it is proposed that the Act be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

- **Statutory Cause of Action for Invasion of Privacy** – The *Privacy Act* should be amended to provide for a statutory cause of action for invasion of privacy. Where there is a reasonable expectation of privacy in all the circumstances, and the act complained of is sufficiently serious to cause substantial offence, an invasion of privacy may be found to have occurred. The circumstances in which an invasion of privacy may occur include where: there has been an interference with an individual's home or family life; an individual has been subjected to unauthorised surveillance; an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; and sensitive facts relating to an individual's private life have been disclosed.

1.6 This Discussion Paper is divided into 10 parts, and contains 64 chapters. It is hoped that those with an interest in a particular area of privacy law will be able to find the relevant information quickly through reference to the Contents, the Part headings and the chapter titles. The ALRC also has prepared *Review of Australian Privacy Law: An Overview*. This document gives an overview of the topics and key proposals in this Discussion Paper. The organisation of this Paper is discussed in greater detail later in this chapter.

Background

ALRC 22

1.7 In April 1976, the ALRC received a wide-ranging privacy reference. Due to particular public concerns at the time, a separate discussion paper and report were completed on access to census records.[11] In the privacy inquiry, two discussion papers were produced—in 1977 and 1980.[12] The final report, *Privacy* (ALRC 22), was tabled in Parliament in December 1983. Discussion of the issues is contained in Volume 1

11 Australian Law Reform Commission, *Privacy and the Census*, DP 8 (1978); Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

12 Australian Law Reform Commission, *Privacy and Publication—Proposals for Protection*, DP 2 (1977); Australian Law Reform Commission, *Privacy and Intrusions*, DP 13 (1980).

and the ALRC's recommendations are contained in Volume 2. Volume 2 also includes draft legislation. Volume 3 contains various appendices.[13]

1.8 The ALRC identified dangers to privacy, including growing official powers, new business practices (such as electronic surveillance, credit reporting and direct marketing), and new information technology. Instead of advocating a single approach to privacy, the ALRC's recommendations targeted a number of different areas in which privacy concerns were identified.

1.9 In formulating its recommendations for legislative reform, the ALRC divided privacy questions into two broad categories—those relating to intrusions, and those relating to information handling. The ALRC subdivided the first category into two broad sub-categories: (1) personal and property intrusions; and (2) spying and intercepting communications. The ALRC noted, however, that the sub-categories 'are not necessarily mutually exclusive'.[14]

1.10 Many of the recommendations relating to information privacy contained in ALRC 22 were subsequently enacted in the *Privacy Act*. In particular:

- a 'permanent statutory guardian for privacy',[15] the Privacy Commissioner, was created;
- statutory privacy principles 'to aid the Privacy Commissioner in the evaluation of complaints about privacy invasion … in respect of … misuse of personal information'[16] were given legislative force;
- access to, and an ability to correct, credit information was provided for; and
- rules governing the use, disclosure and security of some forms of personal information were implemented.

1.11 In IP 31, the recommendations in ALRC 22 relating to intrusions, and significant developments in the intervening period, were outlined.[17] The scope of the current Inquiry is not as broad as ALRC 22,[18] however major advances in information technology have greatly expanded the contexts and concerns about information privacy that are dealt with in this Inquiry. Generally, intrusions only will be reviewed in this

13 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Appendix B, Bibliography on the Concept of Privacy; Appendix C, Tables of Commonwealth and ACT Legislation Conferring Powers of Arrest and Detention, Entry and Search, and Access to, and Production of, Information; Appendix D, Overseas Information Privacy Laws; Appendix E, Laws Regulating Interception of Oral and Written Communication; Appendix F, Course of the Inquiry.

14 Ibid, [1093].

15 Ibid, xliii.

16 Ibid, xliii.

17 See, Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [1.12]–[1.40].

18 See discussion of the scope of this Inquiry below.

Inquiry if they fall within the scope of information collection, use and disclosure. For example, how a marketer obtains a telephone number resulting in an unsolicited telephone communication may fall within the scope of the Inquiry; the intrusion itself does not. If, however, legislative initiatives authorising intrusions, or legislation designed to control unsolicited communications,[19] are inconsistent with the provisions of the *Privacy Act*, and the ALRC's proposals for reform of that Act, such initiatives will be considered.

1.12 Further, to the extent that the intrusion constitutes an invasion of privacy, the proposed statutory cause of action may apply. The cause of action is discussed in detail in Chapter 5.

OECD Guidelines

1.13 On 23 September 1980, the Council of the Organisation for Economic Co-operation and Development (OECD) adopted guidelines governing the protection of privacy and transborder flows of information (OECD Guidelines).[20] The OECD Guidelines were developed to facilitate the harmonisation of national privacy legislation of OECD member countries, and, while upholding human rights, to prevent interruption in the international flow of personal information.[21]

1.14 Eight basic principles of national application are set out in Part Two of the OECD Guidelines:[22]

> **Collection Limitation Principle**—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Data Quality Principle**—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> **Purpose Specification Principle**—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

---

19 The *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) are examples of legislation designed to control unsolicited communications.

20 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

21 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [602]. Levin and Nicholson note that the OECD Guidelines were the product of the Council of Europe's efforts, immediately after its inception in 1949, to address the issue of personal information in 'the aftermath of World War II and its horrors': A Levin and M Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) 2 *University of Ottawa Law and Technology Journal* 357, 374.

22 The full text of the OECD Guidelines can be found at <www.oecd.org>.

Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle—An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.

1.15 The OECD Guidelines, and subsequent models to facilitate transborder data protection, are discussed in detail in Part D.

Privacy Act

1.16 Initially, the *Privacy Act* applied exclusively to the Commonwealth public sector. Public sector agencies are required to comply with IPPs, which are similar, but not identical, to the OECD Guidelines. The Act was amended shortly after its enactment 'to deal with government data-matching activities and the activities of credit

providers and was also extended to cover the Australian Capital Territory public sector'. [23]

1.17 In 2000, amendments to the *Privacy Act* established a separate set of privacy principles, known as the National Privacy Principles (NPPs), which apply to the private sector.[24] The IPPs and the NPPs are discussed in greater detail in Part D. A general overview of the *Privacy Act* is provided in Chapter 3.

The scope of the Inquiry

Terms of Reference

1.18 The Terms of Reference are reproduced at the beginning of this Discussion Paper. The ALRC is directed to focus on the extent to which the *Privacy Act* and related laws continue to provide an effective framework for protection of privacy in Australia. The Attorney-General of Australia, the Hon Philip Ruddock MP, identified four factors as relevant to the decision to initiate the Inquiry:

- rapid advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which privacy should be protected by legislation;
- the expansion of state and territory legislative activity in areas relevant to privacy; and
- emerging areas that may require privacy protection.

1.19 During the course of the Inquiry, the ALRC is directed to consider:

- relevant existing and proposed Commonwealth, state and territory laws and practices;
- other recent reviews of the Privacy Act;
- current and emerging international law and obligations in the privacy area;
- privacy regimes, developments and trends in other jurisdictions;

---

23 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.54]. The credit reporting provisions are discussed in detail in Part G.

24 *Privacy Amendment (Private Sector) Act 2000* (Cth), which came into effect on 21 December 2001.

- any relevant constitutional issue;
- the need of individuals for privacy protection in an evolving technological environment;
- the desirability of minimising the regulatory burden on business in the privacy area; and
- any other related matter.

1.20 The ALRC is directed to identify and consult with relevant stakeholders, including the OPC, relevant state and territory bodies and the Australian business community. The ALRC is also directed to ensure widespread public consultation. The ALRC is asked to provide a final Report to the Attorney-General by 31 March 2008.

Related privacy references

1.21 The Victorian Law Reform Commission (VLRC), the New South Wales Law Reform Commission (NSWLRC) and the New Zealand Law Commission (NZLC) are currently working on privacy references. The Commissions and the ALRC will produce separate consultation papers and final reports; however, the ALRC will work closely with the other Commissions during the course of this Inquiry.

VLRC privacy reference

1.22 In March 2002, the VLRC was asked to examine two issues of public concern relating to privacy: workers' privacy and privacy in public places.[25] As is noted below, the inquiry into workers' privacy has been completed.[26] The VLRC has now embarked on its inquiry into surveillance in public places, and intends to release a Consultation Paper later in 2007.

Workplace privacy

1.23 Apart from the issue of whether employee records should be exempt from the provisions of the *Privacy Act*,[27] the ALRC does not propose in this Inquiry to deal with the specific issue of workplace privacy. The ALRC has been advised that the Standing Committee of Attorneys-General (SCAG) is considering the issue, with a particular focus on workplace surveillance (including email and internet monitoring), covert surveillance practices, surveillance and monitoring outside of work, and genetic testing in the workplace, including the taking of bodily samples. Currently, key stakeholders

---

25 Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004), [1.1]. The Terms of Reference can be found at <www.lawreform.vic.gov.au>.

26 See Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005); Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004); Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002).

27 The use and disclosure of workers' personal information is discussed in Ch 36.

are being consulted about potential options for reform. The ALRC believes that addressing these issues in this Inquiry would duplicate unnecessarily the work being undertaken by SCAG.

1.24 The SCAG review follows the completion by the VLRC in 2005 of its final report on workplace privacy. This VLRC report considered surveillance, monitoring, physical and psychological testing, searching of workers and the collection, use and disclosure of workers' personal information.[28] The VLRC's final report included a draft Workplace Privacy Bill.

NSWLRC privacy reference

1.25 On 11 April 2006, the NSWLRC was asked by the Attorney General of New South Wales to inquire into and report on whether existing legislation in New South Wales provides an effective framework for the protection of the privacy of an individual. In undertaking the review, the NSWLRC is to consider:

- the desirability of privacy protection principles being uniform across Australia;
- the desirability of a consistent legislative approach to privacy in the *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Protection Act 2002* (NSW), *State Records Act 1998* (NSW), *Freedom of Information Act 1989* (NSW) and *Local Government Act 1993* (NSW);
- the desirability of introducing a statutory tort of privacy in New South Wales; and
- any related matters.

1.26 The NSWLRC is also directed to liaise with the ALRC and other relevant Commonwealth, state and territory agencies.

1.27 In May 2007, the NSWLRC released the first of the consultation papers to be published during the course of its inquiry. Consultation Paper 1, *Invasion of Privacy* (NSWLRC CP 1), addresses the desirability of introducing a statutory cause of action for invasion of privacy in New South Wales, and puts forward for consultation proposals for the introduction of such a cause of action. The NSWLRC intends to release a second consultation paper on the remaining aspects of its inquiry in late 2007.

---

28 See Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005); Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004); Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002).

A final report should be completed in early 2008. NSWLRC CP 1 is considered in detail in Chapter 5.

NZLC privacy reference

1.28 The NZLC privacy review will proceed in four stages. Stage one 'is a high level policy overview to assess privacy values, changes in technology, international trends, and their implications for New Zealand law'. In this stage the NZLC will, in conjunction with the ALRC, conduct a survey of international trends. In stage two, the NZLC 'will consider whether the law relating to public registers requires systematic alteration as a result of privacy considerations and emerging technology'. In stage 3, 'the Commission will consider and report on the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy'. A review and update of the *Privacy Act 1993* (NZ) will constitute stage 4.[29] The Terms of Reference for the NZLC privacy review do not specify a reporting date for the projects.

Defining 'privacy'

1.29 It has been suggested that privacy can be divided into a number of separate, but related, concepts:

> **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection';
>
> **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
>
> **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
>
> **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.[30]

1.30 The issues to be covered in this Inquiry, as the preceding discussion illustrates, do not fall neatly into one concept, but the primary focus will be on information privacy.

1.31 The recognition of a general right to privacy warranting legal protection is a relatively modern phenomenon.[31] While the genesis of modern legal academic discussion of the topic is generally acknowledged to be Samuel Warren and Louis

---

29 New Zealand Law Commission, *Review of Privacy* (2006) <www.lawcom.govt.nz/ProjectGeneral.aspx?ProjectID=129> at 1 August 2007. All four stages are described in detail in the Terms of Reference, which can be found on the NZLRC's website.

30 D Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments* Privacy International <www.privacyinternational.org/survey/phr2000/overview.html> at 30 July 2007.

31 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 465.

Brandeis's article, 'The Right to Privacy' published in the *Harvard Law Review* in 1890,[32] widespread debate, particularly in the United States, only commenced in the 1960s[33] and subsequent decades.[34]

1.32 Writing in 1980, Professor Ruth Gavison argued that the modern concern for the protection of privacy can be attributed primarily to

> a change in the nature and magnitude of threats to privacy, due at least in part to technological change … Advances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed.[35]

1.33 Other factors, according to Gavison, include the advent of tabloid journalism, and the 'tendency to put old claims in new terms'.[36]

1.34 In ALRC 22, the ALRC indicated that the chief threats to privacy in Australia included:

> *Growing Official Powers*. The powers of increasing numbers of public officials to intrude into the lives and property of Australians are growing.
>
> *New Business Practices*. New intrusive practices have developed in recent years, such as electronic surveillance, credit reporting and direct marketing.
>
> *New Information Technology*. The computerisation of personal information has enormous advantages, but it also presents Australian society with new dangers, now well documented and understood.[37]

1.35 As evidenced by the Terms of Reference for this Inquiry, all of these factors resonate with equal, if not greater, force today.

---

32 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

33 See, eg, R Prosser, 'Privacy' (1960) 48 *California Law Review* 383; E Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962; C Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475. This is not to suggest an absence of legal discourse between the late 19th century and the 1960s. For example, see the articles cited in E Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962, n 4. See also J Stephen, *Liberty, Equality, Fraternity* (1967 ed, 1873), 160.

34 See, eg, R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421; A Samuels, 'Privacy: Statutorily Definable?' (1996) 17 *Statute Law Review* 115; L Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' (1997) 28 *Metaphilosophy* 259; D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087.

35 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 465. See also, D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 135–136; M Jackson, *Hughes on Data Protection in Australia* (2nd ed, 2001), 10.

36 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 466.

37 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), xli.

1.36 Why is privacy considered important? What is the nature of the legal 'right' requiring protection? Professor Roger Clarke suggests that the importance of privacy has a psychological, sociological, economic and political dimension.

> **Psychologically**, people need private space. This applies in public as well as behind closed doors and drawn curtains …
>
> **Sociologically**, people need to be free to behave, and to associate with others, subject to broad social mores, but without the continual threat of being observed …
>
> **Economically**, people need to be free to innovate …
>
> **[P]olitically**, people need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy.[38]

1.37 The answer to the second question is more difficult. Despite the best efforts of legal scholars, the term 'privacy' eludes a universally accepted definition.[39] In ALRC 22 it was noted that 'the very term "privacy" is one fraught with difficulty. The concept is an elusive one'.[40] As Professor J Thomas McCarthy noted:

> It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.[41]

1.38 In ALRC 22, the ALRC adopted a definition of the term 'privacy' that 'stayed as close as possible … to the ordinary language concept'.[42] This approach has been criticised. Senator Brett Mason suggests that, in this regard, ALRC 22 'is stronger on the practical application of legal rules and remedies to certain privacy issues than it is on theoretical analysis'.[43] He concludes that 'the ordinary language concept of "privacy" … does not necessarily inform a sensible legal right'.[44]

1.39 Mason, like McCarthy, goes on to argue that 'privacy' 'has no core that survives normative analysis'.[45] According to Mason:

> Privacy represents a political or ideological claim. It is a justification or a rallying cry for political debate—just like 'freedom' or 'equality'. Privacy is the respectable

---

38 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 30 July 2007. See also, E Barendt, 'Privacy and Freedom of Speech' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 11, 30–31.

39 L Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' (1997) 28 *Metaphilosophy* 259. One commentator suggests that a reason the legal definition of privacy is so elusive is due to the fact that 'privacy has generally much more to do with politics than with law': B Mason, *Privacy Without Principle* (2006), xii.

40 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [19].

41 J McCarthy, *The Rights of Publicity and Privacy* (2nd ed, 2005), [5.59]. See also, D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 479.

42 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [20].

43 B Mason, *Privacy Without Principle* (2006), 40.

44 Ibid, 41.

45 Ibid, 79.

> umbrella under which diverse political claims seek shelter. But privacy has no core concern or concerns capable of informing a legal right nor principled policy decision making.[46]

1.40 Professor James Whitman suggests that 'there is no such thing as privacy as such'.[47] Comparing American, French and German approaches to privacy, Whitman maintains that:

> Americans and Europeans certainly do sometimes arrive at the same conclusions. Nevertheless, they have different starting points and different ultimate understandings of what counts as a just society … American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity. There are certainly times when the two bodies of law approach each other more or less nearly. Yet they are constantly pulled in different directions, and the consequence is that these two legal orders really do meaningfully differ: Continental Europeans are consistently more drawn to problems touching on human dignity, while Americans are consistently more drawn to problems touching on the depredations of the state.[48]

1.41 Whitman argues that at the core of the European approach to privacy law is 'the right to control your public image—rights to guarantee that people see you the way you want to be seen'.[49] By contrast, the conceptual core of the American right to privacy is, according to Whitman, the 'right to freedom from intrusions by the state, especially in one's own home'.[50]

1.42 Whitman emphasises that the differences between American and European privacy law are comparative, not absolute.[51] It is possible to argue that 'protecting privacy means both safeguarding the presentation of self and inhibiting the investigative and regulatory excesses of the state'.[52] The differences, however, are real.

1.43 Martin Abrams makes a similar observation when he notes that:

> Privacy law is culturally based. Privacy is considered a fundamental human right in Europe, highly regarded with pragmatic interest in the United States, and is only

---

46 Ibid, 80.

47 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1221.

48 Ibid, 1163. See also, R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 569.

49 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1161.

50 Ibid, 1161. The origins of the 'conceptual core', according to Professor Whitman, is the Fourth Amendment—the right against unlawful search and seizures: Ibid, 1212.

51 Ibid, 1203.

52 Ibid, 1219.

> beginning to emerge as a topic in Asia. What works in one country or region doesn't always work in the other.[53]

1.44 This Inquiry has been directed by its Terms of Reference to focus specifically on 'matters relating to the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia'. In the context of information privacy, Professor Margaret Jackson has noted that 'one may query whether it is possible to advance a discussion of the adequacy of the law as a regulator of information privacy if one does not define the privacy interests at risk'.[54]

1.45 Consequently, there may be some utility in attempting to ascertain, if not a 'core' or precise definition of universal application, an understanding of the way the term 'privacy' is being used in the context of this Inquiry. To achieve this objective, the ALRC invited recognised experts to a workshop to discuss the issue. This discussion was useful in articulating the best approach to adopt when tackling the elusive concept of privacy.[55]

Towards a working definition

1.46 Gavison suggests that 'privacy' is 'a term used with many meanings',[56] giving rise to two important questions.

> The first relates to the *status* of the term: is privacy a situation, a right, a claim, a form of control, a value? The second relates to the *characteristics* of privacy: is it related to information, to autonomy, to personal identity, to physical access? Support for all of these possible answers can be found in the literature.[57]

1.47 As a first step in coming to terms with the concept of 'privacy', it is important to recognise that the international community accords privacy the status of a human right through such key documents as the *Universal Declaration of Human Rights*,[58] and the ICCPR.[59] Australia signed the ICCPR on 18 December 1972 and ratified it on 13 August 1980. While 'the rights and obligations contained in the ICCPR are not incorporated into Australian law unless and until specific legislation is passed implementing the provisions',[60] the recognition of privacy as a human right in the

---

53 M Abrams, 'Privacy, Security and Economic Growth in an Emerging Digital Economy' (Paper presented at Privacy Symposium, Institute of Law China Academy of Social Science, 7 June 2006), 18.

54 M Jackson, *Hughes on Data Protection in Australia* (2nd ed, 2001), 6.

55 The workshop participants included Professor Des Butler; Professor Roger Clarke; Professor David Kinley; Mr David Lindsay; Associate Professor Megan Richardson; and Dr Greg Taylor.

56 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 424.

57 Ibid, 424.

58 Article 12 provides: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks': *United Nations Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948).

59 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

60 *Dietrich v The Queen* (1992) 177 CLR 292, 305.

ICCPR lends support to the argument that such recognition in domestic law is warranted.

1.48 Recently enacted domestic human rights legislation also recognises privacy as a basic human right. For example, s 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) provides:

> **Privacy and reputation**
>
> A person has the right—
>
> (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; …

1.49 The *Human Rights Act 2004* (ACT) contains an almost identical provision.[61] While such instruments include privacy in the list of rights accorded the status of a 'human right', they do not define the term, nor do they delineate the extent to which its scope intertwines with other freedoms, rights and interests.[62]

Status of privacy

1.50 Dealing first with the *status* of the term 'privacy' in an Australian context, the VLRC's *Workplace Privacy: Issues Paper* proposed that 'privacy can be expressed as a right, and that this *right* to privacy can then form the basis for determining what are legitimate *interests* in privacy'.[63] The VLRC formulated a working definition of privacy in terms of what the right to privacy encompasses, namely the right:

- 'not to be turned into an object or thing'; and
- 'not to be deprived of the capacity to form and develop relationships'.[64]

1.51 In *R v Broadcasting Standards Commission ex parte BBC,* Lord Mustill attempted to define the essence of privacy.

> To my mind the privacy of a human being denotes at the same time the personal 'space' in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is

61 *Human Rights Act 2004* (ACT) s 12.

62 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 30 July 2007.

63 Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002), xii (emphasis in text).

64 Ibid, [2.38]. Based on this working definition, the VLRC suggested that 'a test of invasion of privacy would be an assessment of the extent to which any particular law or practice has the effect of depriving people generally of [the right not to be reduced to an object and the right to relationships]': Ibid, [2.49].

> damaged both by the violation and by the demonstration that the personal space is not inviolate.[65]

1.52 Put another way, privacy may be viewed as the bundle of interests that individuals have in the personal sphere free from interference from others.[66] In this formulation, the use of the term 'interest' rather than 'right' is intentional. While privacy is a 'right' in a legal sense, for definitional purposes, the word 'interest' may be more accurate. A right is always an interest, even if not all interests are accorded the status of legal rights.

1.53 It is important to bear in mind that privacy interests unavoidably will compete, collide and coexist with other interests. For example, privacy often competes with freedom of expression, a child's right to protection, etc. To ensure equal protection of the same interests in others, no interest, even one elevated to the status of a human right, is absolute.[67]

1.54 The Community Services Ministers' Advisory Council's submission to the Inquiry highlights the practical importance of the recognition of competing interests.

> Privacy is an important individual right. However, this does not stand alone: people also have other rights (to shelter, safety and care) and sometimes the exercise of rights on behalf of one person can have negative consequences for another person. Community services departments and agencies, with duty of care and statutory obligations to protect the vulnerable, are constantly seeking to mediate between competing rights and obligations.[68]

1.55 In a different context, in *McKennitt v Ash* Eady J noted when discussing the tension between freedom of expression and the privacy rights of an individual:

> It is clear that [in the United Kingdom] there is a significant shift taking place as between, on the one hand, freedom of expression for the media and the corresponding interest of the public to receive information, and, on the other hand, the legitimate expectation of citizens to have their private lives protected … Even where there is a genuine public interest, alongside a commercial interest in the media in publishing articles or photographs, sometimes such interests would have to yield to the individual citizen's right to the effective protection of private life.[69]

1.56 Ascertaining the appropriate policy to deal with the tension between competing interests is the challenge facing judges, legislators and law reformers. It follows from the above discussion that the status accorded to privacy, and in particular the status accorded to privacy in international and domestic human rights instruments, means that

---

65 *R v Broadcasting Standards Commission ex parte BBC* [2001] QB 885, [48].

66 See eg R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 30 July 2007.

67 C Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475, 478. See also *Privacy Act 1988* (Cth) s 29(a).

68 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

69 *McKennitt v Ash* [2005] EMLR 10, [57].

privacy interests will usually take precedence over less fundamental interests, such as economic choice and opportunity.[70]

1.57 For example, an argument for greater access to personal information based on reduced cost to data custodians, or customer convenience will generally not tilt the balance in favour of reduced privacy protection. An argument that the use of personal information will lead to an increase in an individual's standard of living may warrant a reduced level of privacy protection, given that standard of living is directly related to the health and wellbeing of an individual or the individual's family—a recognised human right.[71]

Characteristics of privacy

1.58 Identifying the characteristics of privacy is conceptually more difficult than ascertaining its status. Professor Daniel Solove suggests that attempts to identify the characteristics of privacy—that is, the common denominators that make things private—is misguided. Solove argues that:

> the top-down approach of beginning with an over-arching conception of privacy designed to apply in all contexts often results in a conception that does not fit well when applied to a multitude of situations and problems involving privacy.[72]

1.59 Solove advocates a more pragmatic, bottom-up, approach.

> We should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them. If privacy is conceptualized as a web of interconnected types of disruption of specific practices, then the act of conceptualizing privacy should consist of mapping the topography of the web. We can focus on particular points of the web. These 'focal points' are not categories, and they do not have fixed boundaries.[73]

1.60 Some critics, however, reject the pragmatic approach. For example, Professor Richard Bruyer argues that:

> Unless a common denominator is articulated, combining conceptions simply perpetuates the piecemeal, haphazard approach to privacy that has marked the privacy landscape so far. Nor will it provide a satisfactory answer for the hard privacy cases as they occur.[74]

1.61 The characteristics of privacy also may have a changing demographic dimension. For example, what 'Builders' and 'Baby Boomers' see as necessarily

---

70 M Abrams, 'Privacy, Security and Economic Growth in an Emerging Digital Economy' (Paper presented at Privacy Symposium, Institute of Law China Academy of Social Science, 7 June 2006), 9.

71 *United Nations Universal Declaration of Human Rights*, GA Res 217A(III), UN Doc A/Res/810 (1948), art 25.

72 D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1099.

73 Ibid, 1130.

74 R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 576.

falling within the 'topography of the web' may not resonate with 'Generations X, Y and Z'.[75] Young people appear much more willing to share personal details, post images and interact with others on internet chat sites.[76] Does this indicate a changing attitude to privacy? This is discussed in greater detail in Chapter 59.

1.62 The pragmatic approach advocated by theorists such as Solove provides a useful template for law reform. Rather than focusing on an overarching definition of privacy—the privacy 'grail' that inevitably will be so general as to be of limited use to policy makers—it makes more sense, using Solove's terminology, to focus on particular points in the web and formulate a workable approach to deal with the disruption.[77] Provided the underlying policy approach is transparent, this focus may be a more useful conceptualisation of privacy than the search for an all encompassing definition.

1.63 Adopting such an approach makes sense in the context of this Inquiry, given that the ALRC has been asked to review an existing piece of legislation, the *Privacy Act*—which deals with information privacy—and to consider emerging areas that may require privacy protection. The 'focal points' of inquiry have largely been delineated by the legislation, and the reform needed to address any disruptions to specific practices can be articulated with reference to the legislation. In the case of emerging areas that require privacy protection, and in particular those areas falling within the scope of the cause of action for invasion of privacy discussed in detail in Chapter 5, the disruption to specific practices can be identified with reference to case law, academic comment and legislation.

Privacy beyond the individual

Background

1.64 Traditionally, privacy law has protected the privacy rights of individuals—that is, 'natural persons'. Some argue that privacy law also should extend to groups, organisations, partnerships, corporations or other collective entities.[78] For ease of reference, the term 'group' is used here to refer to all such collective entities.

---

75 For a discussion of the age limits of the generational categories, see Part I.

76 L Weeks, 'See Me, Click Me: The Publizen's Life? It's an Open Blog. The Idea He May be Overexposed? LOL', *Washington Post* (online), 23 July 2006, <www.washingtonpost.com>.

77 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 485–486.

78 See, eg, C Doyle and M Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237. Also, the OECD Guidelines note that some members suggested the possibility of extending the Guidelines to legal entities such as corporations and associations: Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [33].

1.65 The *Privacy Act* explicitly confers protection on 'individuals'.[79] Section 6(1) defines 'individual' to mean 'a natural person'.[80] The omission of groups from the ambit of the Act was deliberate, reflecting the rejection in ALRC 22 of the notion of 'corporate privacy'.[81] The ALRC justified this position by reference to art 17 of the ICCPR,[82] the approach taken in most foreign privacy legislation and the ALRC's Terms of Reference.[83] The rejection of corporate privacy also reflects the policy position of the OECD.[84]

1.66 The decision to limit the Act's protection to individuals is reflected in the Preamble to the *Privacy Act*, which makes reference to human rights, and specifically to those guaranteed in the ICCPR. The Preamble also refers to Australia's obligations at international law 'to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence' and to protect 'privacy and individual liberties'.

1.67 In IP 31, the ALRC asked whether it was appropriate to amend the Act to accommodate some form of 'collective' or 'group' right to privacy, applicable to groups such as: (a) Indigenous or other ethnic groups; or (b) commercial entities.[85]

1.68 There are three ways in which legislative privacy protection can apply to groups. First, privacy protection can apply where an individual suffers a breach of his or her privacy as a consequence of the individual's membership of a group. In this situation, the individual's membership of the group does not prevent a claim based on the protection afforded by the *Privacy Act*.

1.69 Secondly, an individual may be permitted to claim privacy rights as a surrogate for an entity that is not a natural person and, consequently, would not otherwise be protected by the Act. Hypothetical examples of this situation are given in ALRC 22:

> Should John Brown, who is entitled to access to his credit record, also be entitled to access to that of John Brown Pty Ltd? Should John Brown Pty Ltd be allowed access to records about John Brown, and about itself? Should Dr Fred Smith, whom everyone in the neighbourhood knows is the real person behind the corporate veil of

79 *Privacy Act 1988* (Cth) pt III, div 1.
80 This is consistent with the definition in Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 1(b).
81 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [27].
82 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).
83 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [27].
84 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [31]–[33].
85 See, Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 1–1.

> Local Medical Services Pty Ltd, be entitled to access to information about both his corporation and himself?[86]

1.70 The ALRC's solution was to provide for a 'flexible test', operating as follows:

> The creation of a corporate or other business structure for a commercial, family or other purpose should not prevent a claim, in the name of a business association, which is in essence one affecting intimate personal interests of an identifiable private individual. A person should have standing in relation to any of the rights and remedies afforded by the draft legislation where he can show that his claim, while nominally concerning an artificial legal person, would affect his personal interests.[87]

1.71 Thirdly, privacy rights could be made to apply directly to a group itself, as distinct from the individuals that are the members of the group. Unlike the circumstances described above, this option is not provided for in the *Privacy Act*. Consequently, in considering reform, there are two related questions: should the *Privacy Act* be amended to provide direct protection to groups; and, if so, which groups should be covered by the Act?

Indigenous and other ethnic groups

1.72 Stakeholders have focused on whether the *Privacy Act* should be amended to respond better to the needs of Indigenous groups—with particular reference to Indigenous groups' traditional laws and customs.[88] While Associate Professor Lee Bygrave has noted that groups constituted by 'sharing certain characteristics, such as … ethnic background' are not generally given express protection in overseas privacy legislation,[89] there is some precedent for explicit privacy protection at common law, in Northern Territory legislation and in regulatory guidance.

1.73 Australian courts generally have responded to the need to maintain the confidentiality of information relating to the traditional laws and customs of Indigenous groups.[90] For example, in *Aboriginal Sacred Sites Protection Authority v Maurice*, the Aboriginal Sacred Sites Protection Authority (ASSPA) challenged the decision of the Aboriginal Lands Commissioner to require an Aboriginal group to produce certain documents as part of a land claim.[91] ASSPA claimed public interest immunity, which it argued derived from the following facts:

> the information in question was gathered under a promise it would be kept confidential … the Aboriginal custodians of the information were bound under

---

86 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [29].
87 Ibid, [29].
88 See, eg, Queensland Government, *Submission PR 242,* 15 March 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
89 L Bygrave, *Submission PR 92,* 15 January 2007.
90 See the discussion of the relevant case law in Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [19.125]–[19.126].
91 *Aboriginal Sacred Sites Protection Authority v Maurice; Re the Warumungu Claim* (1986) 10 FCR 104.

> Aboriginal law and custom to keep the information confidential … production and disclosure in the land claim proceedings would cause dismay and resentment … for the future the flow of information might reasonably be expected to be greatly reduced; and, the standing and working of the Sacred Sites Authority would be gravely prejudiced.[92]

1.74 The Aboriginal Lands Commissioner decided that the documents should be disclosed, but only in a very limited manner: in closed court and to a limited number of named persons who could only use the information in relation to the land claim proceedings. The Full Court of the Federal Court of Australia agreed with this approach, giving some limited protection to the privacy of this information, which was of particular importance to the Aboriginal group in question.[93]

1.75 The *Information Act 2002* (NT) also provides some direct protection for the information privacy of Indigenous groups. Section 50(1) sets out a general requirement that government information be made publicly available, with an exemption where 'it is not in the public interest to disclose the information'. Section 56 then provides a trigger for this exemption in respect of 'privacy and cultural information':

> (1) Information may be exempt under section 50 if disclosure of the information would—
>
> (a) be an unreasonable interference with a person's privacy; or
>
> (b) disclose information about an Aboriginal sacred site or Aboriginal tradition.
>
> (2) Disclosure of information may be an unreasonable interference with a person's privacy even though the information arises from or out of the performance of a public duty.

1.76 It is worth noting that the National Health and Medical Research Council (NHMRC) advises that those conducting research involving humans must consider the 'privacy, confidentiality and cultural sensitivities of participants and, where relevant, of their communities'.[94] Where appropriate, researchers are encouraged to engage 'properly interested parties' such as 'formally constituted bodies, institutions, families or community elders' in planning research projects.[95] In particular, the ethical acceptability of research involving Aboriginal and Torres Strait Islander people may depend upon evidence of support from the relevant communities or groups participating in the research.[96]

---

92 Ibid, 107.
93 Ibid.
94 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [1.10].
95 Ibid, [2.2.13].
96 Ibid, ch 4.7.

Corporations and commercial entities

1.77 Some have suggested that the *Privacy Act* should be extended to protect the putative privacy rights of corporations, arguing that the reason that a right to privacy traditionally has been limited to natural persons is that privacy has been inextricably, but erroneously, linked to autonomy and dignity.[97] Shorn of this link, they see no reason why the same privacy rights enjoyed by natural persons should not be extended to corporations.[98]

1.78 If adopted, this would amount to a very significant extension of the *Privacy Act*. It would also involve departing from the policy approach underlying the Act, and would require a fundamental re-conceptualisation of privacy in Australian law. Privacy is, in law, considered a *human* right—that is, a right that only may be claimed by humans.

1.79 The answer to the question of whether to extend privacy law to provide direct protection of groups will depend, at least in part, on how the jurisdiction in question conceptualises privacy. The vast majority of jurisdictions do not attempt to protect the 'privacy rights' of groups.[99]

1.80 In the United States, for example, the purpose of privacy law has traditionally been seen as 'protecting the individual and not social relationships'.[100] Professor William Prosser's *Restatement of the Law on Torts* sees privacy as denoting 'a personal right, peculiar to the individual whose privacy is invaded'.[101] Reasons for excluding corporations from the protection of US privacy law are that: corporations lack emotional traits; there is insufficient judicial precedent on the issue; and corporations have alternative remedies available to them.[102] Moreover, the rights of collective entities—especially commercial entities—may sometimes resemble privacy rights, but they are not the same, and are therefore subject to a different regime of protection:

> A corporation, partnership or unincorporated association has no personal right of privacy. It has therefore no cause of action for [breach of privacy]. It has, however, a limited right to the exclusive use of its own name or identity in so far as they are of use or benefit, and it receives protection from the law of unfair competition. To some limited extent this may afford it the same rights and remedies as those to which a private individual is entitled …[103]

---

97 C Doyle and M Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237, 246–250.

98 Ibid, 250.

99 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 179, 192–198.

100 N Richards and D Solove, *Privacy's Other Path: Recovering the Law of Confidentiality* (1997) 96 *Georgetown Law Journal* <ssrn.com/abstract=969495>, 50.

101 *Restatement of the Law, 2nd, Torts 1977* (US), § 652I(a).

102 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 193.

103 *Restatement of the Law, 2nd, Torts 1977* (US), § 652I(c).

1.81 Bygrave has pointed out, however, that the data protection laws of some jurisdictions, such as Austria, Italy, Argentina and Switzerland, expressly protect collective entities.[104] The South African Law Reform Commission (SALRC) also has expressed a preliminary view that privacy law should provide some protection to both types of legal person (that is, natural persons and artificial entities, such as corporations). This view was based on four main grounds:

> a) The submissions received were mostly in favour of including juristic persons in the protection of information privacy legislation.
>
> b) Internationally few countries provide privacy protection for juristic persons. However, there seems to be a movement towards broader protection.
>
> c) In terms of sec 8(4) of the Constitution a juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the right and the nature of the juristic person.
>
> d) In each case one would have to ascertain whether appropriate circumstances exist for companies to rely on to protect their privacy interests.[105]

1.82 The SALRC acknowledged, however, that it would be inappropriate to provide the same *level* of protection to collective entities as is afforded to natural persons.[106]

Submissions and consultations

Groups generally

1.83 A large number of stakeholders opposed any legislative extension of privacy rights to groups.[107] Relatively few stakeholders were in favour of such a reform.[108] Many stakeholders observed that privacy is a fundamental *human* right, which is based on protecting dignity and autonomy—characteristics that only individuals possess. As such, it was argued that privacy rights cannot logically be extended to groups.[109] Given

---

104 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 179–180.

105 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), [3.4.23].

106 Ibid, [3.4.8].

107 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Law Society of New South Wales, *Submission PR 146,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

108 See, Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; L Bygrave, *Submission PR 92,* 15 January 2007.

109 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Confidential, *Submission PR 165,* 1 February

that the constitutional foundation of the *Privacy Act* is partly reliant on the fact that it implements art 17 of the ICCPR, the Office of the Information Commissioner Northern Territory expressed a concern that any extension of the Act to protect groups might undermine its constitutional validity.[110]

1.84 Bygrave argued, however, that although 'much of the literature on privacy and its value is almost exclusively concerned with the interests of individual natural/physical persons', privacy need not be viewed through that prism. He stated:

> It is fairly easy to establish that the core principles of the *Privacy Act* are *logically* capable of being extended to protect data on collective entities. Further, it is fairly easy to establish that collective entities are capable of sharing most, if not all, of the interests of data subjects which the *Privacy Act* directly or indirectly safeguards …[111]

1.85 Bygrave counselled against treating 'collective entities … as an undifferentiated mass' because they do not all 'play the same economic, political, legal and social roles, nor have the same goals and resources'.[112] He concluded that, on balance, all countries should seriously consider giving collective entities 'at least some data protection rights', based on the following factors:

> First, the basic principles, rules and rationale of data protection laws are conceptually capable of servicing the interests of collective entities. Secondly, giving collective entities data protection rights can be of practical assistance to them and to the individuals who constitute them. Concomitantly, in many situations where the data protection interests of a collective entity are injured, there can also be injury to the individuals behind the entity. Thirdly, extending coverage of data protection laws to data on collective entities can enhance, in sum, the general transparency of data processing operations, thus promoting a diffusion of knowledge for the benefit of wider society. Fourthly … giving data protection rights to collective entities can expand the possibility of hindering development of control mechanisms facilitating the misuse of power and undermining the bases of pluralistic, democratic society. Finally, giving data protection rights to collective entities (at least those that are organised) does not necessarily:
>
> 1) increase such entities' ability to maintain operational secrecy to the detriment of the general public interest;
>
> 2) weaken the ability of individuals to exercise their own data protection rights;
>
> 3) force collective entities to disclose sensitive business information to their competitors;
>
> 4) overburden data protection authorities; overburden collective entities (as data controllers); or

---

2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Law Society of New South Wales, *Submission PR 146,* 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

110 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

111 L Bygrave, *Submission PR 92,* 15 January 2007 (emphasis in original).

112 Ibid.

5) significantly hinder transborder flows of collective entity data.[113]

Indigenous and other ethnic groups

1.86 A large number of stakeholders opposed extending privacy law to provide specific protection to Indigenous or other ethnic groups.[114] The Office of the Information Commissioner Northern Territory was concerned that such an extension could be used in the name of a group, but 'against the interests of individual group members'.[115]

1.87 One stakeholder submitted that any extension of the Act, if it were limited to Indigenous groups, would be inconsistent with the protection afforded to other cultural groups and it could cause difficulties for agencies in fulfilling their statutory duties.[116] The OPC submitted that such an extension would cause a number of practical problems. For example, it would be difficult to determine which ethnic groups should be afforded additional privacy protection.[117]

1.88 The Australian Government Department of Health and Ageing submitted that such an extension of the Act is unnecessary because the privacy principles already recognise cultural sensitivities adequately

> by requiring the reasonable expectations of the individual concerned to be taken into account when using or disclosing personal information for secondary purposes. Any 'cultural sensitivity' would be one of the matters to be considered in weighing up whether the individual would reasonably expect his or her personal information to be used or disclosed.[118]

1.89 Some stakeholders supported extending privacy law to provide specific protection to Indigenous or other ethnic groups.[119] The Centre for Law and Genetics stated that such an expansion would be consistent with the 'underlying ethical rationale

---

113 Ibid, citing L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 297.

114 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

115 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

116 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

117 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

118 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

119 Queensland Government, *Submission PR 242,* 15 March 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

for privacy protection, which is based in notions of human dignity and autonomy'.[120] The Arts Law Centre of Australia and the National Association for the Visual Arts suggested that privacy law could be used to protect Indigenous culture and intellectual property, by protecting:

- the rights of Indigenous communities to maintain secrecy of Indigenous knowledge and other cultural practices;
- protection of Indigenous sites, including sacred sites;
- control of and access to recordings of cultural customs and expressions, knowledge and skills; and
- protection of secret sacred knowledge.[121]

1.90 Some stakeholders submitted that other methods should be explored to protect the privacy rights of Indigenous groups.[122] In particular, a number of stakeholders supported the creation of privacy protocols, and argued that they should be adopted widely.[123] For example, SBS stated that its Codes, Independent Indigenous Protocols and 1997 policy document, *The Greater Perspective*, all encourage 'respect for Indigenous culture and heritage, recognition of Indigenous cultural and intellectual property rights, maintenance of cultural integrity and respect for cultural beliefs, and respect for Indigenous individuals and communities'.[124] These documents

> include guidelines on consulting with Indigenous groups, and the need to take unique cultural considerations into account when creating content with Indigenous participants. The application of these protocols allow[s] for more positive collaborations with Indigenous communities, rather than the creation of a rigid framework which could serve to silence legitimate voices.[125]

1.91 SBS also did not oppose the introduction of a narrow exemption along the lines of s 56 of the *Information Act 2002* (NT).[126] As discussed above, this provision aims to protect Indigenous sacred sites.

Corporations and commercial entities

1.92 A large number of stakeholders opposed extending privacy law to protect corporations and other commercial entities.[127] Several stakeholders pointed out that

---

120 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

121 Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007. This submission was supported by National Association for the Visual Arts, *Submission PR 151,* 30 January 2007.

122 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; SBS, *Submission PR 112,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

123 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; SBS, *Submission PR 112,* 15 January 2007.

124 SBS, *Submission PR 112,* 15 January 2007.

125 Ibid.

126 Ibid.

127 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007; Australian Privacy Foundation,

corporate and commercial entities can use other laws, such as breach of confidence and intellectual property, to protect their information.[128]

1.93 It was suggested that such an extension would lead to commercial entities operating less transparently.[129] One stakeholder stated that this would inhibit proper corporate governance.[130] The Australian Competition and Consumer Commission submitted that such an extension could allow some corporate entities to 'delay or distract when subject to investigation or other enforcement action'.[131]

1.94 While generally opposed to the extension of privacy law beyond natural persons, the Australian Bankers' Association submitted that, given incorporated entities are no longer able to protect their reputation through defamation, 'arguably a limited right of privacy should be accorded to corporations in relation to the disclosure of defamatory material harmful to the reputation of corporations'.[132]

1.95 Some stakeholders suggested that it may be appropriate to extend privacy law to protect corporations and other commercial entities.[133] Although noting that a small, but significant, number of jurisdictions protect the privacy rights of collective entities such as corporations, Bygrave suggested that this is partly the result of the 'pre-existing legal traditions' in those jurisdictions. He noted that a 'fundamental premise of the Austrian, Swiss and South African legal systems, for example, is that legal persons are to be treated as far as possible in the same way as natural persons'.[134]

ALRC's view

1.96 In the ALRC's view, the *Privacy Act* should not be extended to provide direct protection for the privacy rights of groups—whether these are Indigenous and other

---

Submission PR 167, 2 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Law Society of New South Wales, *Submission PR 146,* 29 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; AXA, *Submission PR 119,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

128 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Law Society of New South Wales, *Submission PR 146,* 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

129 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Confidential, *Submission PR 165,* 1 February 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

130 Confidential, *Submission PR 165,* 1 February 2007.

131 Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007.

132 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

133 W Caelli, *Submission PR 99,* 15 January 2007; L Bygrave, *Submission PR 92,* 15 January 2007.

134 L Bygrave, *Submission PR 92,* 15 January 2007.

ethnic groups, or commercial entities such as corporations. In coming to this view, it was necessary to consider separately whether the Act should be extended in respect of Indigenous and other ethnic groups, and whether it should be extended in respect of commercial entities.

Indigenous and other ethnic groups

1.97 None of the submissions received by the ALRC expressed concerns about the information privacy of any ethnic or cultural groups other than Indigenous groups. At this stage of the Inquiry, the ALRC has concentrated on Indigenous groups as it seems that this is the area of greatest concern. There are, therefore, two questions that need to be addressed here:

- Does the *Privacy Act* provide the necessary level of protection to the information privacy rights of Indigenous groups?

- If not, what is the most appropriate method for achieving this goal? In other words, should legislation such as the *Privacy Act* be amended, or is it more appropriate to use another method?

1.98 The ALRC acknowledges that, under the traditional laws and customs of Indigenous groups, particular information may be subject to restrictions. For example, under such laws and customs, certain information only may be viewed or disclosed to a defined category of people—such as the women of a particular Indigenous group.[135] Another example is that it is often contrary to the traditional laws and customs of Indigenous groups to broadcast the name or image of an Indigenous person who is deceased.[136]

1.99 This raises a question of categorisation. On one view, such laws and customs relate to the information privacy rights of particular Indigenous people, because the information in question is intimately connected to the identity, dignity and autonomy of those people—individually, collectively or both. On another view, these rules more closely resemble intellectual property.[137] For example, it was asserted in argument in *Western Australia v Ward* that Indigenous cultural knowledge of land is 'akin to a new species of intellectual property'.[138]

1.100 The inescapable problem, however, is that these rules do not fit neatly within the Anglo-Australian legal system's traditional conceptualisations of privacy and intellectual property. Such was the case in *Ward* where Kirby J noted, albeit in obiter, that 'the established laws of intellectual property are ill-equipped to provide full

---

135 See, eg, *Wilson v Minister for Aboriginal & Torres Strait Islander Affairs* (1996) 189 CLR 1.

136 See, eg, Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.3.1].

137 See, eg, S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 23.

138 See *Western Australia v Ward* (2002) 213 CLR 1, [59] (Gleeson CJ, Gaudron, Gummow and Hayne JJ), [582] (Kirby J).

protection of the kind sought'.[139] There are many reasons for this disjuncture, beyond obvious differences in the relevant underlying norms. For example, the ALRC has previously noted the widespread view that 'the "knowledge" of members of an [Indigenous] group … is an important component of [Indigenous] traditional laws and customs, in contrast with the Anglo-Australian legal system'.[140] Unlike Anglo-Australian law, for some Indigenous groups, the knowledge aspect of law can be confidential or private.[141] Similarly, the traditional laws and customs of Indigenous groups often delineate between individual and group rights in a way that differs from the Anglo-Australian legal system. It has been observed, for example, that:

> Indigenous legal systems revolve around group rights and group control, whereas the Australian legal system has developed out of a more individualistic tradition, with greater emphasis on personal rights and freedoms.[142]

1.101 There is, therefore, at least an argument that the *Privacy Act* does not adequately protect certain types of information connected with Indigenous groups. Assuming this to be the case, it is then necessary to identify the appropriate solution to this problem.

1.102 As a preliminary point, it should be noted that the ALRC is not persuaded by the assertion of some stakeholders that amending the *Privacy Act* to provide direct protection for the privacy rights of Indigenous groups would be problematic because it would involve unfairly discriminating *in favour* of Indigenous groups. Without detracting from the universality of human rights, there is relatively broad acceptance that particular rights can attach to members of a group of people united by, for example, ethnic origin or religion.[143] It is generally recognised that the individuals comprising certain groups may have needs that are peculiar to those groups. This may result from a group suffering historical discrimination or disadvantage, or it may flow from the particular cultural beliefs or requirements of a group.[144]

1.103 Australian law has long recognised that, in order to ensure that all members of the community enjoy substantive equality, it is sometimes necessary to make laws that are targeted towards individuals who share particular characteristics.[145] For example,

---

139 Ibid, [582].

140 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [19.101].

141 See, eg, the discussion in H McRae, G Nettheim and L Beacroft, *Indigenous Legal Issues* (1997), 133–134.

142 Ibid, 136.

143 This is exemplified in instruments such as Africa's principal human rights treaty, the *African Charter on Human and Peoples' Rights*, 27 June 1981, OAU Doc CAB/LEG/67/3 rev 5, (entered into force generally on 21 October 1986). The Preamble to the Charter recognises that 'fundamental human rights stem from the attributes of human beings which justifies their national and international protection and on the other hand that the reality and respect of peoples' rights should necessarily guarantee human rights'.

144 See, eg, D Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd ed, 2002), 13–14.

145 See, eg, R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000), [12.23].

the *Racial Discrimination Act 1975* (Cth) permits the adoption of 'special measures', which operate as follows:

> Special measures taken for the sole purpose of securing adequate advancement of certain racial or ethnic groups or individuals requiring such protection as may be necessary in order to ensure such groups or individuals equal enjoyment or exercise of human rights and fundamental freedoms shall not be deemed racial discrimination, provided, however, that such measures do not, as a consequence, lead to the maintenance of separate rights for different racial groups and that they shall not be continued after the objectives for which they were taken have been achieved.[146]

1.104 Nevertheless, for the following reasons, the ALRC's considers that it is not appropriate to amend the *Privacy Act* to provide direct protection for the privacy rights of Indigenous groups. First, the Act is premised on the proposition that privacy is a human right and this is reflected in the Preamble, which makes reference to human rights, and especially to the ICCPR. This means that individual members of groups—in this case, members of Indigenous groups—should have their particular privacy needs accommodated. It does not follow, however, that a group should itself be able to claim the protection of the Act in isolation from the individuals that make up that group. As noted in submissions and consultations, such an extension could result in a group asserting privacy rights in a way that conflicts with the interests of individual members of the group.

1.105 Secondly, it should be noted that the vast majority of stakeholders opposed extending the Act's protection to directly cover Indigenous groups. Instead, there is a view that there are other, more appropriate, methods of dealing with this issue. One such method could be to reform Australian intellectual property law, but that issue falls outside the Terms of Reference for this Inquiry.

1.106 In the ALRC's view, the most appropriate means of fostering greater protection of information that is of particular significance to members of Indigenous and other ethnic groups in Australia is for the OPC to encourage and assist agencies and organisations to create publicly available protocols that respond to the privacy needs of these groups. Though generally 'expressed in mandatory language', such protocols are 'primarily ethical in nature'. They articulate 'levels of behaviour which indigenous people and communities expect of outsiders dealing with indigenous material'.[147] Such protocols often suggest ways of protecting the 'honour and dignity' of Indigenous people that are portrayed in the media.[148]

---

146 See *Racial Discrimination Act 1975* (Cth) s 8(1), incorporating *International Convention on the Elimination of all Forms of Racial Discrimination*, 7 March 1966, [1975] ATS 40, (entered into force generally on 4 January 1969), art 1(4).

147 S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 24.

148 See L Bostock, *The Greater Perspective: Protocol and Guidelines for the Production of Film and Television on Aboriginal and Torres Strait Islander Communities* (1997) SBS <www20.sbs.com.au/sbscorporate/media/documents/5315sbs_booklet.pdf> at 17 July 2007, 23.

1.107 An important benefit of adopting such protocols is that this allows the obligations set out in the *Privacy Act* to remain relatively high level, avoiding an overly prescriptive approach.[149] This, in turn, helps the Act to retain its flexibility, allowing it to be applied in a broad range of circumstances. Moreover, such a solution encourages data collectors to consult and negotiate with the relevant members of an Indigenous group before handling information that is culturally sensitive.[150]

Corporations and commercial entities

1.108 The ALRC reaffirms the view expressed in ALRC 22 that the *Privacy Act* should not be extended to provide direct protection to corporations and other commercial entities. First, as already discussed, the *Privacy Act* is premised on the notion that privacy is a human right. It is inconsistent with the fundamental approach of Australian privacy law to try to extend the protection of a human right to an entity that is not human.[151] Furthermore, there are more appropriate avenues for protecting the information rights of commercial entities than through privacy law. Consequently, there seems no valid reason to risk distorting the theoretical basis of the *Privacy Act* by making such a change.

1.109 Secondly, such an extension of the Act would also risk undermining some of the fundamental principles of commercial law. This problem is particularly acute in relation to corporations, which are obliged to operate in a relatively transparent way. Moreover, part of the rationale for adopting the structure of a corporation to pursue a particular activity is precisely to create a barrier between the identity of the corporation and the identity of the persons who establish, run and own it. To assign rights to the corporation would require a choice: either those rights must be assigned to the corporation itself—which would make it necessary to re-conceptualise some fundamental aspects of human rights law; or one must 'pierce the corporate veil', assigning those rights to the persons behind the corporation—which would make it necessary to re-conceptualise some aspects of corporations law.

1.110 Thirdly, while accepting that commercial entities have rights and interests that, in some respects, resemble privacy rights, privacy law is not the most appropriate vehicle by which to vindicate those rights and interests. In particular, intellectual

---

149 See Proposal 15–1 and accompanying text.

150 S Gray, 'Imagination, Fraud and the Cultural Protocols Debate: A Question of Free Speech or Pornography' (2004) 9 *Media & Arts Law Review* 23, 35; Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.3.1]; T Janke and N Guivarra, *Listen, Learn and Respect: Indigenous Cultural Protocols and Radio* (2006) Australian Film Television and Radio School, 17; L Bostock, *The Greater Perspective: Protocol and Guidelines for the Production of Film and Television on Aboriginal and Torres Strait Islander Communities* (1997) SBS <www20.sbs.com.au/sbscorporate/media/documents/5315sbs_booklet.pdf> at 17 July 2007, 25.

151 See, R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000), 3; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226–227 (Gleeson CJ), 258 (Gummow and Hayne JJ), 279 (Kirby J). Callinan J was more equivocal on this point: see 326–327.

property and breach of confidentiality are better tailored to the needs of such entities. Moreover, the *Privacy Act* already provides some protection for sole traders and other such commercial entities where the distinction between the commercial entity and the individual is deliberately much less pronounced.[152]

1.111 Fourthly, extending the *Privacy Act* in this way would radically alter the Act's scope and its objectives.[153] While generally supportive of such an extension of the Act, Bygrave has stated:

> Whether or not the basic principles of [a jurisdiction's data protection] laws *should* be extended to protect collective entity data can only be determined for a particular country on the basis of a consideration of the *need* for extending such protection.[154]

1.112 As noted above, the vast majority of stakeholders opposed such a significant change to these fundamental tenets of the Act. This fact, coupled with the other points noted above, reinforce the ALRC's view that such an extension of the *Privacy Act* is neither necessary nor desirable.

Proposal 1–1 The Office of the Privacy Commissioner should, either on its own motion or where approached in appropriate cases, encourage and assist agencies and organisations, in conjunction with Indigenous and other ethnic groups in Australia, to create publicly available protocols that adequately respond to the particular privacy needs of those groups.

Organisation of this paper

1.113 This Discussion Paper is organised into 10 parts. Part A deals with introductory matters, such as the foregoing discussion of the definition of the word 'privacy', an overview of privacy regulation in Australia,[155] a discussion of the *Privacy Act*,[156] models for achieving national consistency,[157] and the introduction into Australian statute law of a cause of action for invasion of privacy.[158]

1.114 Major proposals for reform in this section include: amended definitions in the *Privacy Act* of 'personal information', 'sensitive information' and 'record';[159] a new

152 Strictly speaking, sole traders are not 'groups' in that they only involve one person: L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 174. See also Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [29].
153 This is also discussed in Ch 3.
154 L Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002), 178 (emphasis in original).
155 Ch 2.
156 Ch 3.
157 Ch 4
158 Ch 5.
159 Proposals 3–4, 3–5 and 3–6.

part of the *Privacy Act* dealing with the personal information of deceased individuals held by organisations;[160] amendments to the *Privacy Act* to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations;[161] the enactment of legislation that regulates the handling of personal information in the state and territory public sectors;[162] and amendment of the *Privacy Act* to provide for a statutory cause of action for invasion of privacy.[163]

1.115 Part B discusses the impact on privacy of rapid advances in information, communication, storage, surveillance and other relevant technologies, and considers how best to accommodate developing technology in a regulatory framework. The impact of the internet, including how the internet has changed the nature of a 'public' space,[164] and the prevalence of identity theft in an electronic environment,[165] are also considered in this part.

1.116 Part C covers how the *Privacy Act* interacts with other federal, state and territory laws, and identifies areas of fragmentation and inconsistency in the regulation of personal information. One of the major proposals for reform contained in this part deals with the access to, and correction of, personal information held by an agency. A proposal is made to amend the *Privacy Act* to provide a new part which deals with requests to access and correct personal information held by agencies.[166]

1.117 Part D outlines the proposed reform of the privacy principles in the *Privacy Act*. A proposal is made to consolidate the existing IPPs and NPPs into one set of principles, the proposed UPPs, applying to both the public and private sector.[167] In addition, proposals are made for substantive amendments to the content of the privacy principles. The chapters are arranged thematically according to the 11 proposed UPPs. In each chapter, there is a brief explanation of how the IPPs and NPPs currently apply, followed by proposals for reform of the specific principle. A draft of the proposed UPPs is set out at the beginning of this Discussion Paper.

1.118 Part E discusses exemptions and partial exemptions to the *Privacy Act*. An exemption applies where a specified entity or a class of entity is not required to comply with the privacy principles that would otherwise be applicable to it. A partial exemption applies where a specified entity or a class of entity is required to comply with either: (1) only some, but not all, of the privacy principles; or (2) some or all of

160 Proposal 3–9.
161 Proposal 4–1.
162 Proposal 4–4.
163 Proposal 5–1.
164 Ch 8.
165 Ch 9.
166 Proposal 12–8.
167 Proposal 15–2.

the privacy principles, but only in relation to certain of its activities. Of particular note are the ALRC's proposals to remove the small business exemption,[168] the employee records exemption,[169] the exemption for political parties and the exemption for political acts and practices.[170]

1.119 Part F is concerned with the OPC. It applies the construct of compliance-oriented regulation to the *Privacy Act*, considering both the regulatory tools provided in the Act and the strategies and approaches adopted by the OPC in using those tools, and examines the appropriate regulatory structure to be adopted by the OPC. The part provides an overview of the Privacy Commissioner's powers and examines the accountability mechanisms which the Commissioner is subject to under the *Privacy Act*; considers the Privacy Commissioner's functions of overseeing and monitoring compliance with the *Privacy Act*; and looks at the Commissioner's powers to issue public interest determinations. One major proposal is to empower the Privacy Commissioner to audit an organisation's compliance with the proposed UPPs, privacy regulations, rules and any privacy code that binds the organisation.[171] Proposals are made to streamline and increase the effectiveness of complaint handling under the *Privacy Act*.[172] The OPC's powers to enforce compliance with the Privacy Act, and in particular whether there needs to be further remedies or penalties available under the Act to enforce compliance, is examined.[173] The issue of data breach notification is considered here, and a model is proposed where notification would be required if specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.[174]

1.120 Part G examines the credit reporting provisions contained in Part IIIA of the *Privacy Act*. The legislative history of these provisions is examined, followed by a discussion of the ALRC's approach to reform. A proposal is made to extend the current system of credit reporting to permit an extension in the categories of personal information able to be collected and disclosed for credit reporting purposes.[175] This part also addresses specific aspects of the credit reporting system, such as collection, use and disclosure of credit reporting information, data quality and security, and rights of access, complaint handling and penalties.[176]

1.121 Part H looks at health information and research, including the need for greater national consistency in health privacy regulation as well as nationwide developments

168 Proposal 35–1.
169 Proposal 36–1.
170 Proposal 37–1.
171 Proposal 44–6.
172 Ch 45.
173 Ch 46.
174 Ch 47.
175 Proposal 51–1.
176 Chs 52–55.

in relation to electronic health information systems.[177] The part examines the way that the *Privacy Act* regulates the handling of health information. Relevant definitions such as the definitions of 'health information' and 'health service' and the additions and exceptions in the privacy principles that relate specifically to health information, are considered. The use of health information in the health services context including the provision of health care and the management, funding and monitoring of health services are also discussed.[178] The special arrangements in place under the *Privacy Act* to allow for the use of personal information in health and medical research are examined, and consideration is given to whether the arrangements should be extended to include the use of personal information in other sorts of research in areas such as criminology and sociology.[179]

1.122 Part I focuses on children, young people and adults requiring assistance. During the early stages of this Inquiry, the ALRC heard anecdotal views that young people think of privacy differently to those of older generations. If this is true, there may be consequences for the development of proposals for privacy that meet the current and future needs of Australians. The attitudes to privacy of children and young people are considered, and major challenges such as online privacy and the taking and uploading of photographs are discussed.[180] The issue of decision making by people under the age of 18 is explored, and proposals are made concerning age of presumed capacity, consent, handling of personal information of persons under the age of 18, education, training and media privacy standards.[181] A test of capacity to give consent, make a request or exercise a right is proposed, and a proposal to introduce into the *Privacy Act* the concept of 'authorised representative' is made.[182] Issues concerning third party assistance with decision making are also discussed in Part I.[183]

1.123 The focus of Part J is on telecommunications, and in particular the interaction between Part 13 of the *Telecommunications Act 1997* (Cth) and the *Privacy Act*. Whether telecommunications-specific privacy legislation is required, and whether Part 13 provides adequate protection of personal information, is explored. The role of the OPC and the Australian Communications and Media Authority under the *Telecommunications Act* is also considered. The Part also considers the *Spam Act 2003* (Cth), *Do Not Call Register Act* 2006 (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth).

177 Ch 56.
178 Ch 57.
179 Ch 58.
180 Ch 59.
181 Ch 60.
182 Ch 61.
183 Ch 62.

Process of reform

Advisory Committee and Sub-committees

1.124 It is standard operating procedure for the ALRC to establish an expert Advisory Committee to assist with the development of its inquiries.[184] In this Inquiry, the Advisory Committee includes current and former Privacy Commissioners; privacy and consumer advocates; privacy professionals; health and social service professionals; academics and practicing lawyers with expertise in privacy, health law and e-commerce; and public and private sector officers with responsibility for privacy. Given the breadth of this Inquiry, the ALRC also has established three Sub-committees of the Advisory Committee in the areas of health privacy, developing technology and credit reporting.[185]

1.125 The Advisory Committee and Sub-committee members have particular value in helping the ALRC identify the key issues and stakeholders, as well as in providing quality assurance in the research and consultation effort. The Advisory Committee and Sub-committees have also assisted with the development of reform proposals and will assist with the formulation of recommendations contained in the final Report. The ultimate responsibility for the final Report and recommendations, however, remains with the Commissioners of the ALRC.

Community consultation and participation

1.126 Under the terms of its constituting Act, the ALRC 'may inform itself in any way it thinks fit' for the purposes of reviewing or considering anything that is the subject of an inquiry.[186] One of the most important features of ALRC inquiries is the commitment to widespread community consultation.

1.127 To date, approximately 200 consultations have been held with individuals, agencies and organisations. The consultations were designed to capture a wide cross-section of interested stakeholders, and included: privacy advocates; academics and lawyers with expertise in privacy; federal, state and territory government departments; state bodies such as the childrens' commissioners of New South Wales, Queensland and Tasmania; the Victorian Government Office of the Health Services Commissioner; federal, state and territory privacy commissioners; privacy commissioners from Canada, the United Kingdom and Germany; business, consumer and health representatives; organisations and agencies representing children and young people; the Access Card Taskforce; the NHMRC; and the Aboriginal Interpreter Service. A list of those with whom the ALRC has consulted is found in Appendix 2 of this Discussion Paper.

---

184 A list of Advisory Committee members can be found in the List of Participants at the front of this publication.

185 Lists of the members of the three sub-committees can be found in the List of Participants at the front of this publication.

186 *Australian Law Reform Commission Act 1996* (Cth) s 38.

1.128 In addition, the ALRC conducted a series of roundtables with individuals, agencies and organisations, on a variety of themes including: credit reporting, exemptions under the *Privacy Act*; the privacy principles; children and young people; and health and research. The ALRC also held a public forum in Melbourne (focusing on consumers and privacy), Sydney (focusing on business and privacy) and Coffs Harbour (focusing on health privacy and research). Finally, youth workshops for those aged 13–25 were held in Sydney, Perth, Brisbane and Hobart.

ALRC National Privacy Phone-in

1.129 On 1 and 2 June 2006, members of the public were invited to contact the ALRC—either by telephone or via the ALRC's website—to share their experiences of privacy breaches and protection. The National Privacy Phone-in attracted widespread media coverage, and in total the ALRC received 1,343 responses.

1.130 The majority of respondents (73%) nominated telemarketing as their main concern.[187] Other prominent issues included:[188]

- handling of personal information by private companies (19%) and government agencies (9%);
- protection of privacy in the internet age (7%);
- identity cards and smart cards (7%); and
- problems accessing and correcting personal information (7%).

1.131 The fact that callers could remain anonymous facilitated frank disclosure. The views expressed included support both for extending and reducing the scope of privacy protection, and provide useful examples of the impact of privacy law in a wide range of circumstances.

Talking Privacy Website

1.132 In early 2007, the ALRC developed a website called 'Talking Privacy', which is accessible from the ALRC's home page. Designed specifically to appeal to young people, the website contains information about the Inquiry, links to further information about privacy law, and encourages young people to send in comments to the ALRC about their privacy issues or experiences. The site also contains information aimed at teachers and students considering law reform or privacy as part of a school curriculum.

---

187 This was possibly influenced by the fact that a number of media stories about the Phone-in focused on telemarketing as a possible concern.

188 Callers were able to nominate more than one concern, which is reflected in the statistics.

1.133 The aim of the Talking Privacy website was to engage young people using a familiar and well-used medium. As at the end of July 2007, the front page of the website had received 3,277 hits. While only a small number of young people had taken the further step of submitting comments for consideration by the ALRC, these were helpful to the Inquiry.

Participating in the Inquiry

1.134 There are several ways in which those with an interest in this Inquiry may participate. First, individuals and organisations may indicate an expression of interest in the Inquiry by contacting the ALRC or applying online at <www.alrc.gov.au>. Those who wish to be added to the ALRC's mailing list for this Inquiry will receive notices, press releases and a copy of this Discussion Paper.

1.135 Secondly, individuals and organisations may make written submissions to the Inquiry in response to this Discussion Paper. There is no specified format for submissions. The ALRC gratefully will accept anything from handwritten notes and emailed dot-points, to detailed commentary on matters related to the Inquiry. The ALRC also receives confidential submissions. Details about making a submission may be found at the front of this Discussion Paper.

1.136 Thirdly, the ALRC maintains an active program of direct consultation with stakeholders and other interested parties. The ALRC is based in Sydney but, in recognition of its national character, consultations will be conducted around Australia during the next phase of the Inquiry. Any individual or organisation with an interest in meeting with the ALRC in relation to the issues being canvassed in the Inquiry is encouraged to contact the ALRC.

Timeframe for the Inquiry

1.137 Two Issues Papers were released before the publication of this Discussion Paper. IP 31 dealt with all matters relevant to the Terms of Reference, with the exception of the credit reporting provisions. Issues Paper 32, *Review of Privacy–Credit Reporting Provisions* (IP 32), dealt with the credit reporting provisions of the *Privacy Act*.

1.138 This Discussion Paper contains a more detailed treatment of the issues raised in both IP 31 and IP 32, and indicates the ALRC's current thinking in the form of specific reform proposals and focused questions. The proposals and questions are put forward for critical examination and to provide a focus for discussion. The Issues Papers and the Discussion Paper may be obtained from the ALRC free of charge on CD-ROM, and may be downloaded free of charge from the ALRC's website, <www.alrc.gov.au>. IP 32 and the Discussion Paper may also be obtained from the ALRC in hard copy.

1.139 The ALRC's final Report, containing the final recommendations, is due to be presented to the Attorney-General by 31 March 2008. Once tabled in Parliament, the Report becomes a public document.[189] The final Report will not be a self-executing document—the ALRC provides advice and recommendations about the best way to proceed, but implementation is a matter for the Government and others.[190]

1.140 The ALRC's earlier Report on privacy contained draft legislation, which formed the basis of the *Privacy Act.* Such draft legislation was typical of the law reform effort in those times. Since then the ALRC's practice has changed, and draft bills are not produced unless specifically called for by the Terms of Reference. This is partly because drafting is a specialised function better left to the legislative drafting experts and partly a recognition that the ALRC's time and resources are better directed towards determining the policy that will shape any resulting legislation. The ALRC has not been asked to produce draft legislation in this Inquiry.

In order to be considered for use in the final Report, **submissions addressing the questions and proposals in this Discussion Paper must reach the ALRC by no later than 7 December 2007**. Details about how to make a submission are set out at the front of this publication.

189 The Attorney-General must table the Report within 15 sitting days of receiving it: *Australian Law Reform Commission Act 1996* (Cth) s 23.

190 The ALRC has a strong record of having its advice followed. About 59% of the ALRC's previous reports have been fully or substantially implemented, about 29% of reports have been partially implemented, 4% of reports are under consideration and 8% have had no implementation to date.

Part A

Introduction

2. Overview—Privacy Regulation in Australia

Contents

Introduction 145
The *Australian Constitution* and privacy 145
Federal regulation of privacy 146
Privacy Act 1988 (Cth) 146
Other relevant federal legislation 147
State and territory regulation of privacy 148
New South Wales 148
Victoria 151
Queensland 154
Western Australia 156
South Australia 158
Tasmania 160
Australian Capital Territory 161
Northern Territory 163
Other relevant state and territory legislation 165
Legislative rules, codes and guidelines 167
Non-legislative rules, codes and guidelines 168

Introduction

2.1 This chapter provides an overview of the regulation of personal information in Australia. The chapter first considers the constitutional framework for privacy laws in Australia. It then provides a brief overview of privacy protection at the federal level and discusses how the *Privacy Act 1988* (Cth) provides for the saving of state and territory privacy laws. The final section outlines the regulation of privacy by the states and territories, and privacy rules, codes and guidelines.

The *Australian Constitution* and privacy

2.2 The *Australian Constitution* establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. It includes a list of subjects about which the Australian Parliament may make laws. That list does not expressly include privacy but this does not mean that the Australian Parliament has no power in relation to privacy.

2.3 The *Privacy Act* was passed in, at least partial, reliance on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs'.[1] The external affairs power enables the Australian Parliament to make laws with respect to matters physically external to Australia;[2] and matters relating to Australia's obligations under bona fide international treaties or agreements, or customary international law.[3] The external affairs power is not confined to meeting international obligations, but also extends to 'matters of international concern'.[4]

2.4 The Preamble to the *Privacy Act* makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the United Nations *International Covenant on Civil and Political Rights*[5] (ICCPR) as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).[6] The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.[7] Chapter 4 further discusses the Australian Parliament's power under the *Australian Constitution* to enact federal privacy laws.

Federal regulation of privacy

Privacy Act 1988 (Cth)

2.5 The principal piece of federal legislation regulating privacy in Australia is the *Privacy Act*. The Act regulates the handling of personal information by the Australian Government, the ACT Government and the private sector. The Act contains a set of 11 Information Privacy Principles (IPPs) that apply to Australian Government and ACT Government agencies, and 10 National Privacy Principles (NPPs) that apply in the private sector. Chapter 3 provides an overview of the *Privacy Act*.

2.6 In general terms, the *Privacy Act* regulates the handling of personal information by the Australian Government, the ACT Government and the private sector. The Act does not regulate the handling of personal information by the state governments or the Northern Territory Government, except to a very limited extent. The *Privacy Act* is expressed to bind the Crown 'in right of the Commonwealth, of each of the States, of

---

1 *Australian Constitution* s 51(xxix). See *Privacy Act 1988* (Cth) Preamble.
2 *Horta v Commonwealth* (1994) 181 CLR 183.
3 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.
4 *Koowarta v Bjelke-Petersen* (1982) 153 CLR 168.
5 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17. See discussion in Ch 4.
6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Part D.
7 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985).

the Australian Capital Territory, of the Northern Territory and of Norfolk Island';[8] however state and territory public sector 'authorities' fall outside the definition of public sector 'agency' and are specifically excluded from the definition of private sector 'organisation'.[9] State and territory authorities include ministers, departments, bodies established or appointed for a public purpose under state and territory law and state and territory courts.[10] Under s 6F of the *Privacy Act*, however, states and territories may request that state and territory authorities be brought into the regime by regulation under the Act.[11]

Saving of state and territory privacy laws

2.7 Section 3 of the *Privacy Act* states:

> It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

2.8 The provision makes clear that the Australian Parliament did not intend to 'cover the field' and to override state and territory laws relating to the protection of personal information if such laws are capable of operating alongside the *Privacy Act*. Section 3 of the *Privacy Act* is discussed in Chapter 4.

2.9 New South Wales (NSW), Victoria and the ACT all have legislation that regulates the handling of personal health information in the private sector. This means that health service providers and others in the private sector in those jurisdictions are required to comply with both federal and state or territory legislation. Part H of this Discussion Paper discusses the issues and problems inherent in this situation. Methods for dealing with these issues are outlined in Chapter 4.

Other relevant federal legislation

2.10 Other federal legislation also regulates the handling of personal information. For example, the *Freedom of Information Act 1982* (Cth) (FOI Act) provides that every person has a right to access documents held by government agencies or Ministers, other than exempt documents. A document is exempt from the freedom of information

---

8 *Privacy Act 1988* (Cth) s 4. Section 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth) makes clear that the private sector amendments were also intended to meet Australia's international obligations, as well as international concerns, relating to privacy.

9 *Privacy Act 1988* (Cth) s 6C(1).

10 Ibid s 6C(3).

11 Ibid s 6F. Only four state authorities have been brought into the regime by regulation. This issue is discussed in detail in Ch 34. In 1994, as part of the transition to self-government, the ACT public service was established as a separate entity from the Australian Government public service. The *Privacy Act* was amended at that time to ensure that ACT public sector authorities continued to be covered by the Act: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).

regime if its disclosure would involve unreasonable disclosure of 'personal information'.[12] This exemption is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own information.[13] The *Archives Act 1983* (Cth) provides a similar exemption.[14]

2.11 The handling of tax file numbers (TFNs) is regulated under various federal Acts including the *Income Tax Assessment Act 1936* (Cth) and the *Taxation Administration Act 1953* (Cth). The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) regulates data-matching using TFNs.

2.12 Various provisions under other federal legislation require or authorise certain acts and practices, including the collection, use and disclosure of personal information. For example, the *Census and Statistics Act 1905* (Cth) and the *Commonwealth Electoral Act 1918* (Cth) require or authorise the collection of large amounts of personal information. Other Acts require or authorise the disclosure of personal information in a range of circumstances, such as the *Australian Passports Act 2005* (Cth), *Corporations Act 2001* (Cth), *Telecommunications Act 1997* (Cth), *Telecommunications (Interception and Access) Act 1979* (Cth) and *Migration Act 1958* (Cth). Federal legislation also contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Federal legislation that regulates the handling of personal information is discussed in detail in Chapters 12 and 13.

State and territory regulation of privacy

2.13 Each Australian state and territory regulates the management of personal information. In some states and territories, personal information is regulated by legislative schemes, in others by administrative regimes.

New South Wales

Privacy and Personal Information Protection Act 1998 (NSW)

2.14 NSW was the first state to enact public sector privacy laws. The *Privacy and Personal Information Protection Act 1998* (NSW) contains a set of privacy standards called Information Protection Principles that regulate the way NSW public sector agencies handle personal information (excluding health information).[15]

---

12 *Freedom of Information Act 1982* (Cth) s 41.
13 Ibid s 41(2).
14 *Archives Act 1983* (Cth) s 33. See discussion in Ch 12.
15 *Privacy and Personal Information Protection Act 1998* (NSW) s 4A. See the discussion of the *Health Records and Information Privacy Act 2002* (NSW) below.

2.15 A number of the Information Privacy Principles are similar to the IPPs in the *Privacy Act*, but they are not identical.[16] There are four major sources of exemptions to the *Privacy and Personal Information Protection Act*: exemptions in the Act;[17] exemptions in regulations;[18] exemptions in a privacy code of practice, made by the Attorney General;[19] and exemptions in a public interest direction made by the NSW Privacy Commissioner.[20]

2.16 The Act provides for the development of privacy codes of practice. A privacy code may modify the application to any public sector agency of one or more of the Information Protection Principles[21] and may exempt a public sector agency or class of public sector agency from the requirement to comply with any of the Information Protection Principles.[22] The Act also provides for privacy management plans.[23]

2.17 The Act establishes the Office of the NSW Privacy Commissioner (Privacy NSW). The NSW Privacy Commissioner has a number of functions, including a complaint-handling function. The NSW Privacy Commissioner must endeavour to resolve complaints by conciliation[24] and may also make written reports on any findings or recommendations made in relation to a complaint.[25]

2.18 Under the existing privacy regime in NSW, there are two avenues of complaint available to individuals who believe that their privacy has been breached. The individual may make a complaint directly to Privacy NSW.[26] Alternatively, those who believe that their privacy has been interfered with by a NSW public sector agency can direct their complaints directly to the agency and request that the agency conduct an internal review of the behaviour that led to the complaint. Privacy NSW is responsible for the oversight of internal reviews.[27] If an individual is not satisfied with the finding of the review or the action taken by the agency in relation to the application, the

16 The *Privacy and Personal Information Protection Act 1998* (NSW) 'adopted with few modifications, the same principles as contained in the Federal Privacy Act': Privacy NSW, *Submission to the Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2005, 17. The *Privacy and Personal Information Protection Act* was enacted before the inclusion of the NPPs in the *Privacy Act*.

17 For example, there are exemptions for law enforcement and investigative agencies: *Privacy and Personal Information Protection Act 1998* (NSW) pt 2 div 3.

18 For example, there are exemptions relating to privacy management plans under the *Privacy and Personal Information Protection Regulation 2005* (NSW) regs 5–7.

19 *Privacy and Personal Information Protection Act 1998* (NSW) ss 29–32.

20 Ibid s 41.

21 Ibid s 30(1).

22 Ibid s 30(2).

23 A privacy management plan must include provisions relating to the development of privacy policies and practices by a NSW public sector agency: Ibid s 33.

24 Ibid s 49.

25 Ibid s 50.

26 Ibid pt 4.

27 Ibid pt 5.

individual may apply to the NSW Administrative Decisions Tribunal for a review of the conduct.[28]

2.19 In 2005–06, 81 complaints were made directly to Privacy NSW.[29] The majority of those complaints were against state government agencies. A significant proportion, however, were also against private organisations and local governments.[30] The most common complaints received by Privacy NSW were about disclosure, surveillance and physical privacy, and collection of information.[31] NSW public sector agencies handled 100 complaints as internal reviews, which were then overseen by Privacy NSW.[32]

Health Records and Information Privacy Act 2002 (NSW)

2.20 The *Health Records and Information Privacy Act 2002* (NSW) implements a privacy regime for health information held in the NSW public sector and the private sector (except small businesses as defined in the *Privacy Act*).[33] The Act allows for individuals to access their health information and establishes a framework for the resolution of complaints regarding the handling of health information.[34]

2.21 The Act contains 15 Health Privacy Principles (HPPs) that outline how health information must be collected, stored, used and disclosed. The HPPs can be grouped into seven areas: collection; storage; access and accuracy; use; disclosure; identifiers and anonymity; and transferrals and linkage.[35] The Act provides for a number of

---

28 Ibid s 55.

29 This is a significant decrease in the number of complaints received the previous year. In 2004–05, Privacy NSW reported that it received 111 complaints: Privacy NSW, *Annual Report 2004–05* (2005), 29. Privacy NSW provides a number of reasons for the drop in complaints: the general public is becoming more aware of the internal review process and increasingly taking the internal review option rather than requesting an investigation by Privacy NSW; agencies have become increasingly familiar with the provisions of the Act; since October 2004, Privacy NSW has been unable to conduct training sessions (training activities raise the profile of the Office and generate further enquiries and requests for advice from the trainees); it is likely that the number of complaints made to a privacy regulator tends to decrease or plateau a few years after the regulator begins operation; it is expected that some individuals did not need to contact Privacy NSW because they had obtained the information they needed from the Privacy NSW website: Privacy NSW, *Annual Report 2005–06* (2006), 18.

30 The NSW Privacy Commissioner also has functions under the *Health Records and Information Privacy Act 2002* (NSW), which regulates both the public sector and private sector.

31 Privacy NSW, *Annual Report 2005–06* (2006), 47.

32 Ibid, 47.

33 See definition of 'private sector person' in *Privacy and Personal Information Protection Act 1998* (NSW) s 4. The Act did not commence until 25 September 2004: *New South Wales Government Gazette (Health Records and Information Privacy Act 2002*), 27 August 2004, 6683.

34 *Health Records and Information Privacy Act 2002* (NSW) s 3.

35 Ibid sch 1. The *Health Records and Information Privacy Act 2002* (NSW) was a result of the recommendations of the Ministerial Advisory Committee on Privacy and Health Information. According to the second reading speech the development of the legislation was also guided by three additional principles: obligations already imposed on service providers and health service providers by existing laws, such as the federal *Privacy Act*; drawing together the best elements of existing privacy legislation at a local, national and international level (in particular the obligations imposed under the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records Act 2001* (Vic)); and to ensure a readily accessible and usable set of principles having due regard to both individual rights and the special needs arising in the management and use of health information. Consistency with the federal *Privacy Act*

exemptions from these principles. For example, the Act does not apply to the Independent Commission Against Corruption, except in connection with the exercise of its administrative and educative functions.[36] Further, the HPPs themselves include exemptions.[37] Some of these exemptions are the subject of statutory guidelines.[38]

2.22 The *Health Records and Information Privacy Act* provides two avenues of complaint to individuals. Parts 3 and 6 of the Act allow individuals to make complaints directly to the NSW Privacy Commissioner.[39] The Act also allows individuals to direct their complaints to the NSW public sector agency for internal review of the conduct that lead to the complaint.[40] In 2005–06, Privacy NSW received 28 complaints relating to health records.[41] NSW public sector agencies handled 20 complaints concerning health records as internal reviews, which were then overseen by Privacy NSW.[42]

Other legislation

2.23 The *Workplace Surveillance Act 2005* (NSW) prohibits covert surveillance of employees in the workplace without appropriate notice. Three categories of surveillance are covered: camera surveillance; surveillance of an employee's use of a work computer; and surveillance of the location or movements of an employee.[43]

Victoria

Information Privacy Act 2000 (Vic)

2.24 The *Information Privacy Act 2000* (Vic) came into force on 1 September 2002. The Act covers the handling of personal information (except health information) in the state public sector in Victoria, and to other bodies that are declared to be 'organisations' for the purposes of Act.[44] Organisations performing work for the Victorian government may also be subject to the Act, depending on the particular contract.[45]

2.25 The Act requires public sector agencies to comply with 10 Information Privacy Principles or have an approved code of practice.[46] The Information Privacy Principles

---

was a particular issue: New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, 2958 (M Egan—Treasurer and Minister for State Development).

36 *Health Records and Information Privacy Act 2002* (NSW) s 17.

37 See, eg, Ibid sch 1, HPP 10(1)(c).

38 See, eg, Privacy NSW, *Health Records and Information Privacy Act 2002 (NSW): Statutory Guidelines on the Management of Health Services* (2004).

39 *Health Records and Information Privacy Act 2002* (NSW) s 58.

40 Ibid pt 3.

41 Privacy NSW, *Annual Report 2005–06* (2006), 47.

42 Ibid, 47.

43 *Workplace Surveillance Act 2005* (NSW) pt 3.

44 *Information Privacy Act 2000* (Vic) s 9.

45 Ibid s 17.

46 Codes of Practice are provided for in Ibid pt 4.

are similar to the NPPs in the *Privacy Act*.[47] The Act contains a number of exemptions, including exemptions in relation to courts and tribunal proceedings, publicly available information and law enforcement.[48]

2.26 The Act establishes the Office of the Victorian Privacy Commissioner. The Victorian Privacy Commissioner's functions include the receipt of complaints about an act or practice that may contravene an Information Privacy Principle or that may interfere with the privacy of an individual.[49] The complaint-handling procedure includes a conciliation process and conciliation agreement. The Victorian Privacy Commissioner also has the power to issue compliance notices in order to enforce the Information Privacy Principles.[50] Unlike the Federal Privacy Commissioner or the Victorian Health Services Commissioner, the Victorian Privacy Commissioner has no power to decide that a breach of privacy has occurred.

2.27 The Office of the Victorian Privacy Commissioner received 82 new complaints in 2005–06.[51] Forty-two of these were against state government departments, 13 were against local councils, 12 were against law enforcement bodies and 10 against statutory authorities. The remaining complaints were against contracted service providers (three complaints) and tertiary institutions (two complaints). The most common complaints related to use and disclosure, data security and the collection of information.[52]

Health Records Act 2001 (Vic)

2.28 The *Health Records Act 2001* (Vic) covers the handling of all health information held by health service providers in the state public sector[53] and the private health sector.[54] The Act contains 11 Health Privacy Principles adapted from the NPPs in the *Privacy Act*.[55] The Act contains a few exemptions to these principles, including

---

47 Ibid sch 1. 'Some modifications to the National Principles have been made to reflect the responsibilities of public sector organisations to promote public interests and be accountable for the expenditure of public funds … In adapting the National Principles under Victorian law it is intended that as much consistency as possible can be maintained with perceptions and practice already operating nationally': Explanatory Memorandum, Information Privacy Bill 2000 (Vic), 7.

48 *Information Privacy Act 2000* (Vic) pt 2 div 2.

49 Ibid s 58.

50 Ibid s 44.

51 This is a significant increase in the number of complaints that were received in the previous year. The Office of the Victorian Privacy Commissioner reported that in 2004–05 it received 50 new complaints: Office of the Victorian Privacy Commissioner, *Annual Report 2004–05* (2005), 20. It stated that this increase is partially due to 21 of the 82 complaints received arising against one organisation out of the same incident: Office of the Victorian Privacy Commissioner, *Annual Report 2005–06* (2006), 23.

52 Office of the Victorian Privacy Commissioner, *Annual Report 2005–06* (2006), 23–25.

53 *Health Records Act 2001* (Vic) s 10.

54 Ibid s 11.

55 'The core elements of the HPPs are consistent with the Information Privacy Principles in Schedule 1 of the *Information Privacy Act 2000*. However, the HPPs specifically address issues pertaining to health information and the provision of health services, and adjusted to have appropriate application to both the public and private sectors': Explanatory Memorandum, Health Records Act 2001 (Vic), 6. *The Health Records Act 2001* (Vic) was designed to operate concurrently with any relevant Commonwealth laws: Victoria, *Parliamentary Debates*, Legislative Assembly, 23 November 2000, 1906 (J Thwaites—Minister for Health).

exemptions for dealing with health information for personal, family or household affairs; for publicly available health information; and for the news media.[56]

2.29 The Office of the Health Services Commissioner administers the Act. An individual may complain to the Office of the Health Services Commissioner about an act or practice that may be an interference with the privacy of the individual.[57] The Commissioner can deal with a complaint in a number of ways, including by: conducting an investigation, by conciliation, a hearing, issuing a compliance notice, or referring a complaint to the Victorian Civil and Administrative Appeals Tribunal.[58] The Office of the Health Services Commissioner closed 253 complaints under the Act in 2005–06. The most common complaints related to access and correction, use and disclosure and data quality.[59]

2.30 The Health Services Commissioner has the power to issue or approve guidelines. These guidelines may lessen the level of privacy protection afforded by a relevant Health Privacy Principle.[60]

Workplace privacy

2.31 In October 2005, the Victorian Law Reform Commission (VLRC) released *Workplace Privacy—Final Report* (2005).[61] The VLRC concluded that significant legislative gaps in the protection of privacy in workplaces required regulation at the state level, and recommended the enactment of workplace privacy legislation and the establishment of a workplace privacy regulator.[62]

2.32 The Victorian Parliament has recently enacted the *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).[63] The Act implements the recommendation of the VLRC report that acts or practices of employers which involve installation, use or maintenance of surveillance devices in relation to their workers should be regulated.[64] The Act amends the *Surveillance Devices Act 1999* (Vic) to make it an offence for an employer knowingly to install, use or maintain an optical surveillance device or listening device to observe, listen to, record or monitor the activities or conversations

56 *Health Records Act 2001* (Vic) pt 2 div 3.
57 Ibid s 45.
58 Ibid pt 6.
59 Victorian Government Office of the Health Services Commissioner, *2006 Annual Report* (2006), 9.
60 *Health Records Act 2001* (Vic) pt 4.
61 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).
62 Ibid, recs 1–65.
63 The Act commenced on 1 July 2007: *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 2.
64 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), rec 31.

of a worker in workplace toilets, washrooms, change rooms or lactation rooms.[65] There are some limited exceptions to this general prohibition.[66]

2.33 The ALRC has been advised that the Standing Committee of Attorneys-General (SCAG) is currently consulting stakeholders about potential options for reform in the area of workplace privacy.

Charter of Human Rights and Responsibilities Act 2006 (Vic)

2.34 The recently enacted *Charter of Human Rights and Responsibilities Act 2006* (Vic) introduces a Charter of Human Rights and Responsibilities for the protection and promotion of human rights in Victoria.[67] Part 2 of the Act sets out a number of human rights including the right of a person not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with. The Act will require statutory provisions to be interpreted in a way that is compatible with the human rights set out under Part 2 of the Act. It will also require public authorities to act in a way that is compatible with those human rights.

Queensland

2.35 In 1997, the Queensland Legislative Assembly Legal, Constitutional and Administrative Committee recommended the enactment of a privacy regime for Queensland based on a set of information privacy principles and the establishment of a Privacy Commissioner.[68] This recommendation has never been implemented. However, Queensland has established an administrative scheme that came into force in 2001 based on the IPPs and the NPPs in the *Privacy Act*. Details of the scheme are provided in Information Standards issued by the Department of Innovation and Information Economy in the *Financial Management Standard 1997* (Qld).[69]

Information Standard 42

2.36 *Information Standard 42—Information Privacy* requires the Queensland state public sector to manage personal information in accordance with a set of Information Privacy Principles adapted from the IPPs contained in the *Privacy Act*. The Information Standard applies to all accountable officers and statutory bodies as defined

---

65 *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 3.

66 Surveillance is permitted: in accordance with a warrant or emergency authorisation or a corresponding warrant or emergency authorisation; in accordance with a law of the Commonwealth; or if required by a condition of a liquor licence granted under the *Liquor Control Reform Act 1998* (Vic): *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 3.

67 The Act, except Divisions 3 (Interpretation of Laws) and 4 (Obligations of Public Authorities) of Part 3, are due to commence on 1 January 2007. Divisions 3 and 4 of Part 3 are due to commence on 1 January 2008.

68 The Committee recognised 'the desirability to have national consistency in privacy protection regimes applicable to both the public and private sectors given the increasingly blurred distinction between those two sectors' and concluded that 'as far as possible, there should be consistency in privacy standards required of the Commonwealth and Queensland public sectors': Legislative Assembly of Queensland—Legal Constitutional and Administrative Review Committee, *Privacy in Queensland*, Report No 9 (1998), [6.1.3].

69 *Financial Management Standard 1997* (Qld) ss 22(2), 56(1).

in the *Financial Administration and Audit Act 1977* (Qld) (including government departments). It also applies to most statutory government owned corporations.[70]

2.37 The requirement for agencies to comply with the Information Standard and guidelines is administratively based. This means that, where conflicting requirements exist, any legislative requirements will supersede compliance with the Information Standard; and compliance is subject to any existing outsourcing arrangements, contracts and licenses.[71]

2.38 The Information Standard provides for two types of exemptions: exemptions relating to bodies that are exempt from all or part of the Information Standard, and personal information that is exempt from the Information Standard.[72]

2.39 The Information Standard contains a number of requirements, including that departments and agencies nominate a privacy contact officer; and that they develop, publish and implement privacy plans to give effect to the Information Privacy Principles.[73] The Information Standard provides that agencies may develop codes of practice that modify the application of the Information Privacy Principles.[74] A set of guidelines has been developed to assist agencies to comply with their obligations under the Information Standard.[75]

2.40 The Queensland Government Department of Justice and Attorney General is responsible for the administration of privacy in Queensland under the Information Standard, which includes initiating whole of government privacy initiatives, providing policy advice and dispensing best practice advisory services to Queensland Government agencies and the community.

Information Standard 42A

2.41 *Information Standard 42A—Information Privacy for the Queensland Department of Health* applies only to that Department and requires health information and personal information to be managed in accordance with National Privacy Principles adapted from the NPPs contained in the *Privacy Act*.[76] A number of principles have been deleted as they do not apply to the Queensland Department of Health or are dealt with under other schemes. For example, NPP 6 has been deleted as the right of access and correction is provided for in the *Freedom of Information Act 1992* (Qld).

---

70 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].
71 Ibid, [1.1].
72 Ibid, [1.2].
73 Ibid, [3.1].
74 Ibid, [1.3].
75 Queensland Government, *Information Standard 42—Information Privacy Guidelines* (2001).
76 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).

2.42 Information Standard 42A is similar to Information Standard 42: it contains the same mandatory requirements, similar exemptions and provides for the development of codes of practice. A set of guidelines has been developed to assist the Department to comply with its obligations under the Information Standard.[77]

Queensland Health Quality and Complaints Commission

2.43 In 2006, the *Health Rights Commission Act 1992* (Qld) was repealed by the *Health Quality and Complaints Commission Act 2006* (Qld). The new Act replaces the Health Rights Commission with the Health Quality and Complaints Commission.

2.44 The Queensland Health Rights Commission was established in 1992 under the *Health Rights Commission Act 1991* (Qld). The Health Rights Commission was responsible for the resolution of health care complaints in Queensland. Although there was no specific provision for privacy complaints under the *Health Rights Commission Act 1992* (Qld), the Health Rights Commission reported that in 2005–06 it received 323 complaints related to 'privacy/discrimination' out of a total of 4465 complaints.[78]

Other legislation

2.45 The *Invasion of Privacy Act 1971* (Qld) requires the licensing and control of credit reporting agents and regulates the use of listening devices.

Western Australia

2.46 The state public sector in Western Australia does not currently have a legislative privacy regime. Some privacy principles are provided for in the *Freedom of Information Act 1992* (WA). This Act provides for access to documents and the amendment of 'personal information' in a document held by an agency that is inaccurate, incomplete, out-of-date or misleading. The definition of 'personal information' is similar to the definition under the *Privacy Act* except that it also includes information about an individual who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.[79]

2.47 Part 4 of the *Freedom of Information Act 1992* (WA) establishes the Information Commissioner. The main function of the Commissioner is to deal with complaints about decisions made by agencies in respect of access applications and applications for amendment of personal information.[80] The Office of the Information Commissioner received 154 complaints in 2005–06. Of these complaints, 135 were for external review of a decision under the *Freedom of Information Act 1992* (WA). External

77 Queensland Government, *Information Standard 42A—Information Privacy Guidelines* (2001).
78 Queensland Health Rights Commission, *Annual Report 2005–2006* (2006), 5, 8.
79 *Freedom of Information Act 1992* (WA) Glossary.
80 Ibid s 63.

review complaints include complaints relating to applications for access to documents and the amendment of personal information under the Act.[81]

2.48 The *State Records Act 2000* (WA) affords some limited protection of privacy. For example, under the Act, no access is permitted to medical information about a person unless the person consents, or the information is in a form that neither discloses nor would allow the identity of the person to be ascertained.[82] However, neither the *State Records Act* nor the *Freedom of Information Act 1992* (WA) deals comprehensively with privacy issues associated with collection, storage and use of personal information by agencies.

Information Privacy Bill 2007

2.49 The Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament on 28 March 2007. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information by the public and private sectors in Western Australia.[83]

2.50 The Bill requires most state public sector agencies, and contractors to public sector agencies, to comply with a set of eight Information Privacy Principles. The Information Privacy Principles draw heavily on the NPPs contained in the *Privacy Act* and on the Information Privacy Principles in the Victorian *Information Privacy Act 2000* (Vic).[84]

2.51 The Bill also requires most public sector agencies, private sector health service providers, and persons or bodies in the private sector who handle health information about individuals, to comply with a set of 10 Health Privacy Principles. The Health Privacy Principles are adapted from, and are consistent with, the *Draft National Health Privacy Code*.[85] They are broadly similar to the general requirements of the NPPs in the *Privacy Act*, but are specifically tailored to the privacy of health information.[86] Under Part 3 Division 2 of the Bill, individuals will be given access to records held by private sector organisations and increased ability to amend their records. This is similar to the power under the *Freedom of Information Act 1992* (WA).

---

81 Information Commissioner Western Australia, *Annual Report 2005–06* (2006), 12–13.

82 *State Records Act 2000* (WA) s 49.

83 A related Bill, the Freedom of Information Amendment Bill 2007 (WA), was introduced on the same day. This Bill provides the Privacy and Information Commissioner with powers to resolve FOI complaints by conciliation.

84 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 March 2007 (J McGinty—Attorney General).

85 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003). See Part H for a discussion of the *Draft National Health Privacy Code*.

86 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 Match 2007 (J McGinty—Attorney General).

2.52 The Act contains a number of exemptions, including for courts and tribunals[87] and publicly available information.[88] Various law enforcement agencies and child protection agencies do not have to comply with certain Information Privacy Principles and Health Privacy Principles.[89] The Bill also provides for Codes of Practice that can derogate from the Information Privacy Principles and the Health Privacy Principles.[90]

2.53 Part 6 of the Bill overrides prohibitions on the disclosure by public sector agencies of personal and health information, whether those prohibitions result from other statutes, the common law, or ethical or professional obligations, provided the disclosure meets certain criteria. These criteria include, for example, that the disclosure is for the purpose for which the information was collected, or that the disclosure falls within certain specified exceptions to the information privacy principle or health privacy principle relating to use and disclosure.

2.54 The Bill establishes the Privacy and Information Commissioner who will replace and expand the role of the current Information Commissioner. The Commissioner's functions and powers include: monitoring and promoting compliance with the Information Privacy Principles and the Health Privacy Principles, reporting to the minister on the legislation, and resolving complaints.[91] The complaint-handling process includes the use of conciliation proceedings.[92] Complaints that are not resolved through conciliation may be resolved by the State Administrative Tribunal.[93]

South Australia

Cabinet Administrative Instruction

2.55 There is no legislation that specifically addresses privacy in South Australia.[94] The South Australian Department of the Premier and Cabinet, however, has issued an administrative instruction requiring its government agencies to comply with a set of Information Privacy Principles based on the IPPs in the *Privacy Act*. *PC012—Information Privacy Principles Instruction* was first issued in July 1989 and then reissued in July 1992.[95]

2.56 The Privacy Committee of South Australia was established in 2001 to oversee the implementation of the Information Privacy Principles in the South Australian public sector and to provide advice on privacy issues. The Committee oversees the

87 Information Privacy Bill 2007 (WA) cl 9.
88 Ibid cl 10.
89 Ibid cl 11. Schedule 2 contains a list of exempt organisations.
90 Ibid cl 15–16, 18–19 and pt 4.
91 Ibid cl 120.
92 Ibid cl 79.
93 Ibid cl 85.
94 There have been recent calls for the introduction of privacy legislation in South Australia. See, eg, 'Democrats Want SA Privacy Commissioner', *ABC News* (online), 6 June 2007, <www.abc.net.au/news>.
95 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

regime and performs a complaint-handling role. The Committee's functions include the referral of written complaints concerning violations of individual privacy received by it to an appropriate authority.[96] The Committee must prepare a report of its activities annually and submit the report to the Minister (currently the Minister for Administrative Services and Government Enterprises). Members of the public who are unsatisfied with the Privacy Committee's response to their complaint are referred to the South Australian Ombudsman for further investigation.[97] The Committee is also able to exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit.[98]

2.57 The ALRC has been informed that State Records of South Australia (State Records), in supporting the Privacy Committee of South Australia, is developing a guideline for matching and sharing personal information. State Records is also examining other opportunities for guidelines and proposed amendments to the Instruction that might improve the protection of privacy within the South Australian public sector. Other projects include the development of a standard under the *State Records Act 1997* (SA) relating to contracting out and the handling of personal information.[99]

Code of Fair Information Practice

2.58 South Australia also has a *Code of Fair Information Practice* based on the NPPs in the *Privacy Act*.[100] The Code applies to the South Australian Department of Health and the Department for Families and Communities.[101]

---

96 Ibid, Schedule. The Committee has reported that in 2005–06 it received four new complaints in addition to six existing complaints. The Committee concluded seven of the 10 complaints: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2004–05* (2005), [3.5].

97 Privacy Committee of South Australia, *Privacy Committee Members' Handbook Version 1.1* (2005), 16.

98 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), Schedule; Privacy Committee of South Australia, *Privacy Committee Members' Handbook Version 1.1* (2005), Appendix 1. The Committee granted two exemptions in 2005–06: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2005–06* (2006), [3.3].

99 State Records of South Australia, *Correspondence*, 13 June 2007. See also Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2005–06* (2006), [3.4.1], [3.4.2].

100 South Australian Government Department of Health, *Code of Fair Information Practice* (2004), Foreword. The Information Privacy Principles are set out in Appendix B. The South Australia Department of Health considered that the NPPs provided an ideal basis for the Code because 'they are generally applicable to the private sector, particularly those organisations which collect, use, store or disclose "sensitive information"—much of the type of data held by the Department of Health and its service providers'. In adopting the NPPs the South Australia Department of Health was attempting to align 'as much as possible to what looks likely to be the model for a nationally consistent scheme for managing personal information': South Australian Government Department of Health, *Code of Fair Information Practice* (2004), 6.

101 South Australian Government Department of Health, *Code of Fair Information Practice* (2004), 7; Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2004–05* (2005), [3.3.1].

Tasmania

Personal Information Protection Act 2004 (Tas)

2.59 The *Personal Information Protection Act 2004* (Tas) regulates the collection, use and disclosure of personal information. The Act applies to 'personal information custodians' including state government agencies, statutory boards, local councils, the University of Tasmania and any body, organisation or person who has entered into a personal information contract with government agencies relating to personal information.[102] A 'personal information contract' is a contract between a personal information custodian and another person relating to the collection, use or storage of personal information.[103]

2.60 The 10 'personal information protection principles' set out in Schedule 1 of the Act are based on the NPPs in the *Privacy Act*. However, aspects of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Information Privacy Act 2000* (Vic) have also been incorporated into the principles.

2.61 The Tasmanian regime is similar to legislation in other jurisdictions in that it contains exemptions for publicly available information and law enforcement information.[104] The obligations in relation to 'employee information', however, are different to the federal and other state and territory regimes in that they allow job applicants and employees to benefit from the privacy obligations imposed on employers.[105] A personal information custodian may also apply to the Minister for Justice for an exemption from compliance with any or all of the provisions of the Act.[106]

2.62 Part 4 of the Act provides for complaints and investigations. Rather than establishing a central body (such as a privacy commissioner) to manage complaints, the Tasmanian Ombudsman either investigates and determines the complaint or refers the complaint to another person, body or authority that the Ombudsman considers appropriate in the circumstances.[107] If, on completion of an investigation of a complaint, the Ombudsman is of the opinion that a personal information custodian has contravened a personal information protection principle, the Ombudsman may make any recommendations the Ombudsman considers appropriate in relation to the subject matter of the complaint.[108]

---

102 See definition of 'personal information custodian': *Personal Information Protection Act 2004* (Tas) s 3.
103 Ibid s 3.
104 Ibid ss 8, 9.
105 Ibid s 10.
106 Ibid s 13.
107 Ibid s 20.
108 Ibid s 22.

Charter of Health Rights

2.63 The *Health Complaints Act 1995* (Tas) requires the Tasmanian Health Complaints Commissioner to develop a *Charter of Health Rights*.[109] A Charter was developed and tabled in Parliament in 1999. The Charter applies to a wide range of health service providers.

2.64 The Charter provides for six rights, including the right to confidentiality, privacy and security.[110] It sets out a range of rights of health service consumers including the right of a consumer: to have his or her personal health information and any matters of a sensitive nature kept confidential; for health service facilities to ensure his or her privacy when receiving health care; and to expect that information about his or her health is kept securely and cannot easily be accessed by unauthorised persons. The Charter also provides that health service providers have the right to discuss the health care and treatment of a consumer with other providers for advice and support if it is in the best interest of the consumer's health and wellbeing.[111]

2.65 The Tasmanian Health Complaints Commissioner administers the Charter.[112] The Tasmanian Health Complaints Commissioner has a number of functions including the receipt, assessment and resolution of complaints.[113] Complaints may be resolved by conciliation and through the use of enforceable agreements between a complainant and health service provider.[114] In 2005–06, the Commissioner reported that she resolved 38 privacy-related complaints out of a total of 663 complaints resolved in that period.[115] The ALRC has been advised that the Charter will be reviewed in late 2007.[116]

Australian Capital Territory

2.66 The ACT public sector complies with an amended version of the *Privacy Act*.[117] The Office of the Privacy Commissioner (OPC) administers the Act on behalf of the ACT government.

---

109 *Health Complaints Act 1995* (Tas) s 17.

110 Tasmanian Government Office of the Health Complaints Commissioner, *Tasmanian Charter of Health Rights and Responsibilities* (2006), 7.

111 Ibid, 7.

112 In Tasmania the same person holds the office of the Ombudsman and the Tasmanian Health Complaints Commissioner.

113 *Health Complaints Act 1995* (Tas) s 6(d) and pt 4.

114 Ibid pt 5.

115 Tasmanian Government Health Complaints Commissioner, Annual Report 2005–06 (2006), 52. However, the category 'Privacy' includes assault, breach of confidentiality, discrimination, failure to ensure privacy, inconsiderate service and unprofessional conduct.

116 Tasmanian Government Health Complaints Commission, *Correspondence*, 12 June 2007.

117 See *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth). For example, the amended version provides that certain reports following the investigation of a complaint by the Privacy Commissioner are to be supplied to the ACT Attorney-General.

Health Records (Privacy and Access) Act 1997 (ACT)

2.67 The *Health Records (Privacy and Access) Act 1997* (ACT) removes health records from the jurisdiction of the OPC. The Act regulates the handling of health records held in the public sector in the ACT and also applies to acts or practices of the private sector. The Act contains 14 privacy principles that have been modified to suit the requirements of health records.[118]

2.68 The Act gives people access to their own health records or any other record to the extent that it contains personal health information.[119] The Act imposes obligations on both the person requesting access to a health record[120] and the person who responds to a request for access.[121] The Act contains a number of exemptions to the general right to access health records. For example, it is a ground of 'non-production' if the record or part of the record does not relate in any respect to the person requesting it.[122]

2.69 The ACT Human Rights Commission administers the Act.[123] Under Part 4, a complaint may be made to the Commissioner on the following grounds: the act or omission contravenes the privacy principles in relation to a consumer; the act or omission is a refusal to give access in accordance with the Act to a health record relating to a consumer; or the act or omission is a refusal by a record keeper of a health record to give access to the health record under the Act.

2.70 The Human Rights Commission commenced on 1 November 2006. The Commission is an independent agency established by the *Human Rights Commission Act 2005* (ACT). The Commission brings together the existing functions of the ACT Human Rights Office and the Community and Health Services Complaints Commissioner. The *Health Records (Privacy and Access) Act* was previously administered by the ACT Community and Health Services Complaints Commissioner. In 2005–06, the Community and Health Services Complaints Commissioner received 25 complaints about access to health records, and 10 complaints about disclosure of personal health information.[124]

Human Rights Act 2004 (ACT)

2.71 Section 12 of the *Human Rights Act 2004* (ACT) provides that all individuals have the right not to have their privacy, family, home or correspondence interfered with unlawfully or arbitrarily or have their reputation unlawfully attacked. The Act also imposes a duty of consistent interpretation in respect of other legislation. Under

---

118 *Health Records (Privacy and Access) Act 1997* (ACT) s 5 and sch 1.
119 Ibid s 10.
120 Ibid s 12.
121 Ibid s 13.
122 Ibid s 14.
123 Ibid s pt 4.
124 ACT Government Community and Health Services Complaints Commissioner, *Annual Report 2005–06* (2006), 40.

the Act, when a court is interpreting an ACT law it must adopt an interpretation 'consistent with human rights' as far as possible.[125]

Northern Territory

Information Act 2002 (NT)

2.72 The Northern Territory has combined its information privacy, freedom of information, and public records laws into a single Act, the *Information Act 2002* (NT). Schedule 2 of the Act contains 10 Information Privacy Principles. The Information Privacy Principles are based on the NPPs in the *Privacy Act*.[126] The Act provides for a number of exemptions to the Information Privacy Principles. For example, the Information Privacy Principles do not apply to publicly available information,[127] or to court or tribunal proceedings.[128]

2.73 The Act also provides for approved codes of practice.[129] A code may specify the manner in which a public sector agency is to apply or comply with one or more of the Information Privacy Principles. A code may also modify an Information Privacy Principle, but only in limited circumstances.[130]

2.74 Part 6 of the Act establishes the Information Commissioner for the Northern Territory. The Information Commissioner may authorise a public sector agency to collect, use or disclose personal information in a manner that would otherwise contravene or be inconsistent with specified Information Privacy Principles.[131] The Commissioner also has the power to issue a notice requiring a public sector organisation to take specified action within a period to ensure that in the future it complies with an IPP or code of practice.[132]

2.75 A person may make a complaint to the Commissioner about a public sector organisation that has collected or handled his or her personal information in a manner that contravenes an Information Privacy Principle, a code of practice or an authorisation; or has otherwise interfered with the person's privacy.[133] The Information Commissioner has the power to conduct a hearing in relation to the complaint and

125 *Human Rights Act 2004* (ACT) s 30(1).
126 Northern Territory, *Parliamentary Debates*, Legislative Assembly, 14 August 2002 (P Toyne—Minister for Justice and Attorney-General).
127 *Information Act 2002* (NT) s 68.
128 Ibid s 69. For other exemptions, see *Information Act 2002* (NT) pt 5 div 2.
129 *Information Act 2002* (NT) ss 72–80.
130 Ibid s 72.
131 Ibid s 81.
132 Ibid s 82.
133 Ibid s 104.

make a number of orders.[134] In 2005–06, the Information Commissioner received five privacy complaints.[135]

Information Privacy Code of Conduct

2.76 The Northern Territory does not have health specific privacy legislation. In 1997, however, the Territory Health Services issued the *Territory Health Services Information Privacy Code of Conduct*.[136] The Code of Conduct includes 11 principles that are based on the IPPs in the *Privacy Act*.[137] The Code covers personally identifiable health information, data collections, staff records, and commercially sensitive information. It is enforceable under the *Public Sector Employment and Management Act* (NT).[138] However, legislative provisions take precedence over the *Code of Conduct*.[139]

Code of Health Rights and Responsibilities

2.77 The *Code of Health Rights and Responsibilities* made under s 104(3) of the *Health and Community Services Complaints Act 1998* (NT), confers a number of rights and responsibilities on all users and providers of health and community services in the Northern Territory.[140] The rights and responsibilities set out in the Code are not absolute—they do not override duties set out in Northern Territory or federal legislation.

2.78 Principle 4 of the Code relates to personal information. It provides that people have a right to information about their health, care and treatment. They do not have, however, an automatic right of access to their care or treatment records. Under the Principle, health service providers may prevent health service users from accessing their records where legislative provisions restrict the right to access information, or the provider has reasonable grounds to consider that access to the information would be prejudicial to the user's physical or mental health. The Principle also provides that health service providers have a responsibility to protect the confidentiality and privacy of health service users.

2.79 The Northern Territory Health and Community Services Complaints Commission handles complaints in relation to non-compliance with the Code. Complaints are administered under the *Health and Community Services Complaints Act 1998* (NT). Under that Act, the Commissioner may resolve complaints by conciliation,[141] and may receive complaints from the Information Commissioner.[142]

---

134 Ibid s 115.
135 Northern Territory Government Office of the Information Commissioner, *Annual Report 2005–06*, 24.
136 Northern Territory Government Department of Health, *Information Privacy Code of Conduct* (1997).
137 Ibid, [1.6].
138 Ibid, [1.3].
139 Ibid, [1.3.2], [1.5].
140 Northern Territory Government Health and Community Services Complaints Commission, *Code of Health Rights and Responsibilities*, 6.
141 *Health and Community Services Complaints Act 1998* (NT) pt 6.
142 Ibid s 25A.

The Health and Community Services Complaints Review Committee may review decisions by the Commissioner.[143] In 2005–06, the Commission reported that it did not receive any complaints relating to access to records, and that it received two complaints relating to 'privacy/confidentiality'.[144]

Proposed health privacy legislation

2.80 In March 2002, the Northern Territory Department of Health and Community Services released a discussion paper, *Protecting the Privacy of Health Information in the Northern Territory*.[145] The discussion paper sought views on the need for the development of health-specific privacy protection for the Northern Territory. The legislation proposed by the discussion paper would apply to public sector organisations only, and consisted of three main elements: the protection of the privacy of an individual's health information in both the public and private sectors in the Northern Territory; the establishment of a right for individuals to access their own health information; and the conferral of jurisdiction on the Health and Community Services Complaints Commissioner to oversee the health privacy regime and to handle and resolve complaints.[146] To date, a final report has not been released.

Other relevant state and territory legislation

2.81 Personal information is also regulated under state and territory legislation that is not specifically concerned with the protection of personal information. Examples of such legislation include legislation that contains secrecy provisions, freedom of information legislation, public records legislation, listening and surveillance devices legislation and telecommunications legislation.

2.82 Legislation in each state and territory includes provisions that place obligations on public sector agencies and individuals in the public sector not to use or disclose certain information. For example, s 9 of the *Public Sector Management Act 1994* (WA) requires all public sector bodies to be 'scrupulous in the use of official information'. Other state and territory legislation includes secrecy provisions. Often these provisions state that the disclosure of certain information is an offence.[147] For example, s 22 of the *Health Administration Act 1982* (NSW) provides that it is an offence to disclose information obtained in connection with the administration of the Act, subject to a number of exceptions.

---

143 Ibid pt 9.

144 Northern Territory Government Health and Community Services Complaints Commission, *Eighth Annual Report 2005–2006* (2006), 68.

145 Northern Territory Government Department of Health and Community Services, *Protecting the Privacy of Health Information in the Northern Territory*, Discussion Paper (2002).

146 Ibid, Ch 8.

147 Other examples of secrecy provisions include *Health Administration Act 1982* (NSW) s 22; *Public Health Act 1991* (NSW) s 75; *Criminal Code 1913* (WA) s 81; *Health Act 1911* (WA) ss 246ZM and 314; *Public Sector Management Act 1995* (SA) s 57; *Public Health Act 1997* (Tas) s 139.

2.83 Each state and territory has freedom of information legislation that enables the public to access information held by that state or territory government. The right of access to information is subject to a number of exceptions. Documents affecting personal privacy of third parties will usually be exempt from the access requirements under the Act or will only be released after a consultation process.[148] Freedom of information legislation also attempts to ensure that records held by the Government concerning the personal affairs of members of the public are complete, correct, up-to-date and not misleading.[149]

2.84 Public records legislation in each state and territory is intended to ensure the effective management of government records and improved record keeping. The legislation provides for public access to records as well as setting out restrictions on access to certain records. Some state and territory public records legislation restricts access to records that contain personal information.[150]

2.85 Some privacy protection is also provided in state and territory legislation regulating the use of listening and other surveillance devices,[151] and telecommunications interception.[152]

2.86 Various state and territory laws regulate the private sector. For example, s 19 of the *Introduction Agents Act 1997* (Vic) regulates the handling of personal information by introduction agencies about their clients. State and territory public health Acts require health service providers, including private health service providers, to collect and record certain information about health consumers with 'notifiable diseases', such as, tuberculosis, Creutzfeldt-Jakob disease and AIDS.[153] State and territory adoption laws contain a range of provisions regulating adoption records held by Government and private adoption agencies, including providing for retention, disclosure and access

148 *Freedom of Information Act 1989* (NSW) s 31 and sch 1 pt 2 cl 6; *Freedom of Information Act 1982* (Vic) s 32; *Freedom of Information Act 1992* (Qld) s 44; *Freedom of Information Act 1992* (WA) s 32; *Freedom of Information Act 1991* (SA) s 26; *Freedom of Information Act 1991* (Tas) s 30; *Freedom of Information Act 1989* (ACT) s 41; *Information Act 2002* (NT) ss 15, 33.

149 *Freedom of Information Act 1989* (NSW) pt 4; *Freedom of Information Act 1982* (Vic) pt 5; *Freedom of Information Act 1992* (Qld) pt 4; *Freedom of Information Act 1992* (WA) pt 3; *Freedom of Information Act 1991* (SA) pt 4; *Freedom of Information Act 1991* (Tas) pt 4; *Freedom of Information Act 1989* (ACT) pt 5; *Information Act 2002* (NT) pt 3.

150 *Public Records Act 1973* (Vic) s 9; *Public Records Act 2002* (Qld) ss 16, 18; *State Records Act 2000* (WA) s 49; *Archives Act 1983* (Tas) s 15; *Territory Records Act 2002* (ACT) s 28.

151 *Listening Devices Act 1984* (NSW); *Surveillance Devices Act 1999* (Vic); *Police Powers and Responsibilities Act 2000* (Qld); *Surveillance Devices Act 1998* (WA); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2000* (NT).

152 *Telecommunications (Interception) (New South Wales) Act 1987* (NSW); *Telecommunications (Interception) (State Provisions) Act 1988* (Vic); *Telecommunications (Interception) Western Australia Act 1996* (WA); *Telecommunications Interception Act 1988* (SA); *Telecommunications (Interception) Tasmania Act 1999* (Tas); *Telecommunications (Interception) Northern Territory Act 2001* (NT).

153 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

to information.[154] State and territory laws that regulate the private sector are discussed further in Chapter 4.

Legislative rules, codes and guidelines

2.87 Legislation other than the *Privacy Act* requires the development of privacy codes or guidelines.[155] For example, s 112 of the *Telecommunications Act* enables bodies and associations in the telecommunications industry to develop industry codes relating to telecommunications activities. In 2003, the Australian Communications Industry Forum released an industry code on calling number display (CND). The Code aims to regulate the manner in which CND is to be offered to customers by suppliers; options that customers have in relation to using or blocking the display of CND information from their services; charges that may apply in relation to enabling or blocking the display of CND information to CND services; and measures to be undertaken by suppliers to ensure that the public is aware of CND services and their implications.[156]

2.88 Another example is codes developed pursuant to s 123 of the *Broadcasting Services Act 1992* (Cth). Under this provision, the industry group responsible for representing various radio and television licensees (that is, commercial, subscription and community broadcasters) must develop a code of practice applicable to that section of the broadcasting industry. Privacy provisions are included in the various broadcasting codes of practice developed by representative industry bodies. In the commercial broadcasting and subscription broadcasting sectors, the privacy provisions relate to news and current affairs programs. In the case of the community broadcasting sector, the privacy provisions relate to all programs. For example, s 2 of the *Commercial Radio Codes of Practice* provides that news programs (including news flashes) broadcast by a licensee must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, unless there is a public interest in broadcasting such information.[157]

2.89 As noted above, a number of state and territory privacy laws provide for the making of codes that may derogate from the privacy principles in the primary legislation. The Attorney General of NSW has approved a number of privacy codes of practice that modify the application of the *Privacy and Personal Information Protection Act 1998* (NSW). For example, the *Privacy Code of Practice for Local*

---

154 See, eg, *Adoption Act 2000* (NSW) ch 8; *Adoption Act 1984* (Vic) pt 6; *Adoption of Children Act 1964* (Qld) pt 4A; *Adoption Act 1988* (SA) pt 2A, pt 3; *Adoption Act 1994* (WA) pt 4; *Adoption Act 1988* (Tas) pt 6; *Adoption Act 1993* (ACT) pt 5; *Adoption of Children Act* (NT) pt 6.

155 For other examples of legislative codes and guidelines see Ch 14.

156 Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2003).

157 Reproduced in Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), Attachment A.

Government has the effect of modifying the application of Part 6 of the *Privacy and Personal Information Protection Act 1998* (NSW) (the 'public register' provisions) and the application of the 12 Information Protection Principles as they apply to local government.[158]

Non-legislative rules, codes and guidelines

2.90 In addition to legislative protection of personal information, organisations will often develop and publish privacy guidelines that are not required by legislation.[159] For example, the private sector provisions of the *Privacy Act* exempt from its ambit acts by media organisations in the course of journalism when the organisation is publicly committed to observing a set of privacy standards.[160] The Australian Press Council (APC) has developed a set of eight privacy standards to regulate the handling of personal information.[161] The Standards relate to the collection, use and disclosure of personal information; quality and security of personal information; anonymity of sources; correction, fairness and balance of media reports; sensitive personal information; and complaint handling. The APC receives and deals with complaints in relation to the Standards.

158 See, eg, Privacy NSW, *Privacy Codes of Practice* <www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipcodes> at 30 July 2007.

159 For other examples of non-legislative codes and guidelines see Ch 14.

160 *Privacy Act 1988* (Cth) s 7B(4).

161 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 30 July 2007. The Standards adopt the *Privacy Act* definition of 'personal information'.

3. The *Privacy Act*

Contents

Introduction 169
Overview of the *Privacy Act* 171
- Agencies and organisations 171
- Acts and practices 171
- Exemptions and exceptions 172
- Information Privacy Principles 174
- National Privacy Principles 175
- Approved privacy codes 175
- Interference with privacy 176
- Credit reporting 176
- Tax file numbers 177
- Privacy Commissioner 177
- Privacy Advisory Committee 181
- Privacy regulations 181

The structure of the Act 182
The name of the Act 184
The objects of the Act 187
- Submissions and consultations 191
- ALRC's view 192

Some important definitions 194
- Personal information 194
- ALRC's view 202
- Sensitive information 206
- Records 215
- Generally available publications 218

Deceased individuals 219
- Submissions and consultations 223
- ALRC's view 226

Introduction

3.1 This chapter provides an overview of the *Privacy Act 1988* (Cth) in its current form and proposes some basic changes. For example, it is proposed that the name of the Act be changed and that an objects clause be included in the Act. The chapter proposes amending some of the key definitions in the Act, such as the definition of

'personal information'. It also proposes that a level of privacy protection be extended to the personal information of deceased individuals.

3.2 The Privacy Bill 1988 was introduced into the Australian Parliament in November 1988[1] by the then Attorney-General, the Hon Lionel Bowen MP. The Bill was in part a response to a number of developments in the 1970s and 1980s including continuing advances in the technology available for processing information.

3.3 The Preamble to the Bill makes clear that the legislation was intended to implement Australia's obligations relating to privacy under the United Nations *International Covenant on Civil and Political Rights*[2] (ICCPR) as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[3] (OECD Guidelines). The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[4] (Council of Europe Convention).

3.4 The Hon Justice Michael Kirby chaired the group of government experts that developed the OECD Guidelines. As Chairman of the Australian Law Reform Commission (ALRC), Justice Kirby also oversaw the production of the three volume report, *Privacy* (ALRC 22), published in 1983.[5] The report included draft legislation, which drew on the OECD Guidelines, and was considered by the Australian Government in developing the Privacy Bill.

3.5 The *Privacy Act*, in its original form, set out the Information Privacy Principles (IPPs), which regulate the handling of personal information by Australian Government departments and agencies. It established the position of the Privacy Commissioner, within the Human Rights and Equal Opportunity Commission. The Act provided guidelines for the handling of individual tax file number (TFN) information in both the public and private sectors following enhancements in the use of this unique identifier in 1988.[6]

3.6 The *Privacy Act* also applies to ACT public sector agencies. In 1994, as part of the transition to self-government, the ACT public service was established as a separate

---

1 A predecessor Privacy Bill was introduced into Parliament in 1986, in association with the Australia Card Bill 1986, but both Bills lapsed with the double dissolution of Parliament in 1987. The Australia Card proposal is discussed further in Ch 27.

2 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

3 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Ch 1.

4 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985).

5 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

6 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth). TFNs are discussed further in Ch 27.

entity from the Australian Government public service. Amendments were made at that time to ensure that ACT public sector agencies continued to be covered by the Act.[7]

3.7 The Act has been substantially amended on a number of occasions. In 1990, the Act was amended to provide safeguards for individuals in relation to consumer credit reporting.[8] These amendments governed the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers.

3.8 In 2000, the Act was amended to extend coverage to private sector organisations more generally.[9] This amendment introduced the National Privacy Principles (NPPs) into the legislation. The NPPs were developed following consultation with business, consumers and other stakeholders.[10] Further amendments in 2000 established the Office of the Privacy Commissioner (OPC) as a statutory authority independent of the Human Rights and Equal Opportunity Commission.[11]

Overview of the *Privacy Act*

Agencies and organisations

3.9 Broadly speaking, the IPPs regulate the activities of Australian Government public sector agencies. 'Agency' is defined to include ministers, departments, federal courts and other bodies established for a public purpose.[12] The NPPs regulate the activities of private sector organisations. 'Organisation' is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust.[13] There are a number of exceptions to, and exemptions from, the definitions of 'agency' and 'organisation'. These are discussed below and in Part E.

Acts and practices

3.10 The *Privacy Act* applies to 'acts and practices', that is, acts done and practices engaged in by agencies or organisations. The Act includes a wide range of exemptions for particular acts and practices discussed briefly below and in more detail in Part E.

3.11 For the purposes of this Discussion Paper, the ALRC distinguishes between the terms 'handling' and 'processing' of personal information. The ALRC uses the term *handling* personal information to refer to all acts and practices in the information cycle

---

7 *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).
8 *Privacy Amendment Act 1990* (Cth). Credit reporting is discussed in detail in Part G.
9 *Privacy Amendment (Private Sector) Act 2000* (Cth).
10 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
11 *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth).
12 *Privacy Act 1988* (Cth) s 6(1).
13 Ibid s 6C.

including collection, use, disclosure, storage and destruction of personal information no matter what mechanism is used. The ALRC uses the term *processing* to refer to electronic processing of personal information. The ALRC notes that the European Union Article 29 Data Protection Working Party recently made the same distinction in its *Opinion 4/2007 on the Concept of Personal Data*.[14]

Exemptions and exceptions

3.12 The *Privacy Act* contains a range of exemptions and exceptions. They are found throughout the Act, in the definition of some terms, in specific exemption provisions and in the IPPs and NPPs themselves. This Discussion Paper distinguishes between exemptions, partial exemptions and exceptions to the requirements set out in the *Privacy Act*. An *exemption* applies where a specified entity or a class of entity is not required to comply with the privacy principles. A *partial exemption* applies where a specified entity or a class of entity is required to comply with either: (1) only some, but not all, of the privacy principles; or (2) some or all of the privacy principles, but only in relation to certain of its activities. An *exception* applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. This distinction is discussed in more detail in Chapter 30.

3.13 The acts and practices of some Australian Government agencies—including the intelligence agencies: the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation and the Office of National Assessments—are completely exempt from the *Privacy Act*.[15]

3.14 Certain acts and practices of other agencies are also exempt. For example, while federal courts fall within the definition of agency for the purposes of the *Privacy Act*, only some acts and practices of federal courts are covered by the Act.[16] Acts and practices in relation to administrative functions such as personnel files, operational and financial records, and mailing lists, for example, are covered.[17] However, acts done and practices engaged in as part of the courts' judicial functions are not covered.

3.15 In relation to the private sector, the definition of organisation specifically excludes many small business operators and registered political parties. Small businesses are defined in the *Privacy Act* as those with an annual turnover of $3 million or less. This exemption was thought necessary to avoid the imposition of unnecessary costs on small business.[18] Some small businesses that pose a higher risk to privacy—for example, small businesses that hold health information and provide

---

14 European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007), 5.

15 *Privacy Act 1988* (Cth) s 7. The exemptions for the defence and intelligence agencies are discussed in detail in Ch 31.

16 Ibid s 7. Courts and tribunals are discussed in detail in Ch 32.

17 *I v Commonwealth Agency* [2005] PrivCmrA 6.

18 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General). The small business exemption is discussed in detail in Ch 35.

health services or those that trade in personal information—are covered by the Act.[19] Other small business operators may choose to opt in to the regime[20] or may be brought into the regime by regulation.[21]

3.16 State and territory public sector authorities fall outside the definition of 'agency' and are specifically excluded from the definition of 'organisation'. States and territories may request, however, that such authorities be brought into the regime by regulation.[22]

3.17 The Act does not apply to personal information being collected, used or disclosed for personal, family or household purposes.[23]

3.18 The *Privacy Act* includes an exemption for employee records. Organisations are exempt in relation to past or present employees if the relevant act or practice is directly related to an employee record and the employment relationship.[24] At the time the private sector amendments were passed, the Attorney-General noted that this type of personal information is deserving of privacy protection but that the issue was more appropriately dealt with in workplace relations legislation.[25] To date, however, the issue has not been effectively dealt with in this way and so employee records in the private sector remain without adequate privacy protection.

3.19 Media organisations are exempt in relation to acts or practices in the course of journalism.[26] A media organisation is an organisation whose activities consist of or include the collection, preparation and dissemination of news, current affairs, information or documentaries. Media organisations can claim the exemption if they have publicly committed to observing published, written standards that deal with privacy in the context of media activities. This exemption is intended to allow a free flow of information to the public through the media.[27]

3.20 Political acts and practices by political representatives, such as parliamentarians, are exempt where those acts and practices relate to the political process. Contractors, subcontractors and volunteers working for registered political parties or political

---

19 *Privacy Act 1988* (Cth) s 6D(4).
20 Ibid s 6EA.
21 Ibid s 6E.
22 Ibid s 6F.
23 Ibid ss 7B(1), 16E.
24 Ibid s 7B(3). The employee records exemption is discussed in detail in Ch 36.
25 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
26 *Privacy Act 1988* (Cth) s 7B(4).
27 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General). The media exemption is discussed in detail in Ch 38.

representatives also may be exempt where their acts or practices are related to the political process.[28]

3.21 The IPPs and NPPs include a number of exceptions. For example, under IPP 6 individuals are entitled to access their own personal information except to the extent that a record-keeper is required or authorised by law to refuse to provide the individual with access. IPP 10 provides that personal information shall not be used for any purpose other than the purpose for which it was collected except in a number of specified circumstances, for example, where the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; the use is required or authorised by law; or the use is necessary to enforce the criminal law. There are similar exceptions relating to the disclosure of information under IPP 11.

3.22 The NPPs contain a range of similar exceptions as well as specific and qualified exceptions for the use of non-sensitive information for direct marketing purposes and the use of health information for medical research.

Information Privacy Principles

3.23 The 11 IPPs are based on the OECD Guidelines.[29] The IPPs are a central feature of the *Privacy Act* and are discussed in detail in Part D. The IPPs require that Australian Government agencies have a lawful purpose for collecting personal information, and that the purpose is related to the functions or activities of the agency.[30] Agencies collecting personal information from individuals must ensure that those individuals are generally aware of the purpose for which the information is being collected, whether the collection is authorised or required by or under law and the agency's usual practices in relation to disclosure of such information.[31] The IPPs require agencies to ensure that information is relevant, up-to-date and complete.[32]

3.24 Agencies must also store information securely[33] and provide information about the type of personal information they hold.[34] Subject to certain exceptions, agencies must provide individuals with access to personal information about them and correct the information they hold to ensure that it is accurate, up-to-date, relevant, complete and not misleading.[35] Agencies must generally seek an individual's permission to use or disclose information for a purpose that is not directly related to the purpose for which it was collected.[36]

---

28 *Privacy Act 1988* (Cth) s 7C. The political exemption is discussed in detail in Ch 37.
29 Ibid s 14.
30 Ibid s 14, IPP 1.
31 Ibid s 14, IPP 2.
32 Ibid s 14, IPP 3.
33 Ibid s 14, IPP 4.
34 Ibid s 14, IPP 5.
35 Ibid s 14, IPP 7.
36 Ibid s 14, IPPs 10, 11.

National Privacy Principles

3.25 The 10 NPPs—developed in consultation with private sector organisations—apply in the private sector where no approved privacy code has been put in place.[37] The NPPs are discussed in detail in Part D. The NPPs require that organisations collect personal information by lawful and fair means and not in an unreasonably intrusive manner. Information must be necessary for one of the organisation's functions or activities and must be collected from the individual concerned, where it is reasonable and practicable to do so.[38] Sensitive information, including health information, may generally only be collected with consent.[39]

3.26 Organisations may only use and disclose personal information for the purpose for which it was collected, except in a number of defined circumstances. For example, an organisation may use personal information for a related purpose if that would be within the reasonable expectations of the individual.[40] Organisations must take reasonable steps to ensure that the personal information they handle is accurate, complete and up-to-date[41] and must protect the information from misuse and loss and from unauthorised access, modification or disclosure.[42] Organisations must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.[43]

3.27 On request, organisations are required to let individuals know what sort of personal information they hold and how they handle that information,[44] and to give individuals access to the information held about them unless particular exceptions apply.[45] There are limits on the use of government identifiers by the private sector,[46] and on transferring personal information overseas.[47] Organisations are also required to have a written privacy policy that sets out how the organisation manages personal information and to make the policy available to anyone who asks for it.[48]

Approved privacy codes

3.28 The *Privacy Amendment (Private Sector) Act 2000* (Cth) introduced Part IIIAA into the *Privacy Act*, which allows private sector organisations and industries to develop and enforce their own privacy codes. Once the Privacy Commissioner

37 Ibid sch 3.
38 Ibid sch 3, NPP 1.
39 Ibid sch 3, NPP 10.
40 Ibid sch 3, NPP 2.
41 Ibid sch 3, NPP 3.
42 Ibid sch 3, NPP 4.
43 Ibid sch 3, NPP 4.
44 Ibid sch 3, NPP 5.
45 Ibid sch 3, NPP 6.
46 Ibid sch 3, NPP 7.
47 Ibid sch 3, NPP 9.
48 Ibid sch 3, NPP 5.

approves a privacy code, it replaces the NPPs for those organisations bound by the code.[49] Codes may also set out procedures for making and dealing with complaints. Such codes must provide for the appointment of an independent adjudicator to whom complaints may be made.[50]

3.29 The aim of amending the Act in this way was to encourage private sector organisations and industries to develop privacy codes of practice.[51] To date, only four codes have been approved by the Privacy Commissioner: the Market and Social Research Privacy Code, the Queensland Club Industry Privacy Code, the Biometrics Institute Privacy Code and the General Insurance Information Privacy Code. The General Insurance Information Privacy Code has since been revoked. Privacy codes are discussed further in Chapter 44.

Interference with privacy

3.30 Part III Division 1 of the *Privacy Act* sets out what amounts to an 'interference with privacy', that is, a breach of the Act that gives grounds for a complaint to the Privacy Commissioner or an independent adjudicator appointed under an approved privacy code. An act or practice by an agency that breaches an IPP is an interference with privacy.[52] An act or practice by an organisation that breaches an NPP or an approved privacy code is an interference with privacy.[53] An interference with privacy may also arise in other areas including: the handling of TFN information, data-matching, and credit reporting.

Credit reporting

3.31 As noted above, the *Privacy Act* was amended in 1990—following public controversy over the credit industry's intention to introduce a system of 'positive' (more comprehensive) credit reporting[54]—to provide safeguards for individuals in relation to consumer credit reporting.[55] In particular, Part IIIA of the Act regulates the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers. The Privacy Commissioner is required to issue a Code of Conduct that, together with Part IIIA, applies privacy protections to the handling of personal credit information.[56] The current Code includes amendments made following a number of reviews and is dated March 1996.[57]

---

49 Ibid s 16A.
50 Ibid s 18BB.
51 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
52 *Privacy Act 1988* (Cth) s 13.
53 Ibid s 13A.
54 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 30 July 2007.
55 *Privacy Amendment Act 1990* (Cth).
56 *Privacy Act 1988* (Cth) s 28A.
57 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 30 July 2007.

3.32 The credit reporting provisions have been the subject of criticism[58] and are considered in detail in Part G.

Tax file numbers

3.33 TFNs are unique numbers issued by the Australian Taxation Office (ATO) to identify individuals, companies and others who lodge income tax returns with the ATO. The *Privacy Act* provides for the making of specific guidelines in relation to the collection, storage, use and security of TFN information relating to individuals.[59] The TFN Guidelines, issued under s 17 of the *Privacy Act*, are legally binding. A breach of the guidelines is an interference with privacy and provides grounds for a complaint to the Privacy Commissioner.[60] Interim Guidelines contained in a schedule to the *Privacy Act* operated until they were replaced with the *Tax File Number Guidelines 1990*. The current guidelines were issued in 1992 and have been amended on a number of occasions.[61]

Privacy Commissioner

3.34 The *Privacy Act* establishes the position of the Privacy Commissioner as an independent statutory officer who is appointed by the Governor-General for a period of up to seven years.[62] The powers and role of the Privacy Commissioner are examined in detail in Part F.

Office of the Privacy Commissioner

3.35 The *Privacy Act* establishes the OPC—consisting of the Privacy Commissioner and his or her staff—as a statutory agency to oversee the implementation of the *Privacy Act*.[63] The Office consists of the following sections:

- the Hotline Section;
- the Compliance Section;
- the Policy Section; and
- Corporate and Public Affairs.

---

58 See, eg, G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

59 TFNs are discussed in detail in Ch 27.

60 Unauthorised use or disclosure of TFNs is also an offence under the *Taxation Administration Act 1953* (Cth). This Act protects all TFNs and not just those of individuals.

61 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).

62 *Privacy Act 1988* (Cth) ss 19–25.

63 Ibid ss 19, 26A.

3.36 The Hotline Section provides assistance to individuals in relation to their rights under the *Privacy Act* and related legislation. It also provides advice to agencies and organisations on how to comply with the Act and related legislation.

3.37 The Compliance Section investigates complaints from individuals against agencies and organisations. It also investigates possible breaches of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and associated Guidelines, the Tax File Number Guidelines and the guidelines in force under the *National Health Act 1953* (Cth). In addition, the section audits agencies, credit providers and credit reporting agencies. Compliance also conducts audits under s 309 of the *Telecommunications Act 1997* (Cth).

3.38 The Policy Section provides guidance and advice to agencies and organisations on privacy issues; examines and makes submissions on proposed legislation; comments on inquiries that have significant privacy implications; and seeks to inform itself of technological and social developments that affect individual privacy. The Corporate and Public Affairs section assists the OPC in communicating with stakeholders through publications, media relations, secretariat support, speech writing, events and the OPC website.[64]

Functions of the Privacy Commissioner

3.39 The Privacy Commissioner's functions are set out in a number of Acts including the *Privacy Act*. Those in the *Privacy Act* include:

- promoting an understanding and acceptance of the IPPs and the NPPs and undertaking educational programs in relation to privacy;
- investigating acts or practices that may breach the IPPs or NPPs, either in response to complaints or on the Commissioner's own initiative;
- auditing the handling of personal information by agencies to ensure that they comply with the IPPs;
- considering and approving privacy codes and reviewing the operation of the codes and decisions of adjudicators appointed under those codes;
- considering legislation that might impact on privacy and ensuring that any adverse effects are minimised;
- undertaking research into and monitoring developments in data processing and computer technology to ensure that any adverse privacy effects of such developments are minimised;

64 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 30 July 2007.

- publishing various guidelines, including binding guidelines, on the development of privacy codes and the use of health information for medical research;[65] and

- providing advice to the Minister and others.[66]

3.40 As noted above, the Privacy Commissioner also has functions under the *Privacy Act* in relation to TFN information and credit reporting. In addition, the Commissioner has responsibilities under the:

- *Data-matching Program (Assistance and Tax) Act 1990* (Cth) in regulating the conduct of Australian Government data-matching programs. The Privacy Commissioner is required to issue guidelines under the Act and has the power to investigate acts or practices that may breach the guidelines;[67]

- *National Health Act 1953* (Cth) in regulating the handling of Medicare and Pharmaceutical Benefits Program claims information. The Privacy Commissioner is required to issue guidelines under the Act and has the power to investigate acts or practices that may breach the guidelines;[68]

- *Crimes Act 1914* (Cth) in regulating the handling of information about spent convictions. Part VIIC of the Act provides for a spent convictions scheme that prevents discrimination against individuals on the basis of certain previous convictions. The Commissioner has the power to investigate complaints about breaches of Part VIIC;[69] and

- *Telecommunications Act 1997* (Cth) in monitoring disclosures of personal information to law enforcement agencies and consulting on industry codes and standards in a range of consumer protection and privacy areas.[70]

3.41 In performing his or her functions, the Privacy Commissioner is required to take certain matters into account, including Australia's international obligations and relevant international guidelines on privacy. The Commissioner is also required to have due regard to the protection of important human rights and social interests that compete

---

65 The guidelines made under ss 95 and 95A of the *Privacy Act* in relation to the use of health information in research are discussed in Ch 58.

66 *Privacy Act 1988* (Cth) s 28A.

67 These guidelines are discussed further in Chs 7 and 44.

68 These guidelines are discussed further in Chs 44 and 56.

69 These functions are discussed further in Ch 44.

70 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 30 July 2007. These functions are discussed further in Ch 63, including the question of whether these functions should be consolidated into the *Privacy Act*.

with privacy such as the free flow of information through the media and the right of government and business to achieve their objectives in an efficient way.[71]

Investigations

3.42 The Privacy Commissioner has the power to investigate on his or her own motion, or in response to a complaint, acts and practices of agencies or organisations that may breach the IPPs or NPPs.[72] In conducting such investigations, the Commissioner can require the production of documents and information, and may also require people to appear and answer questions.[73] The Commissioner may examine such witnesses on oath or affirmation.[74]

3.43 The Privacy Commissioner may make a determination where there has been a breach of the IPPs or NPPs.[75] The Commissioner may determine that the conduct must not be repeated; that the agency or organisation must take action to redress the loss or damage caused; or that the complainant is entitled to a specified amount of compensation. The Commissioner may also dismiss the complaint or decide to take no further action. Such determinations, however, are not binding as between the parties. If it becomes necessary to enforce the determination, action must be taken in the Federal Court or the Federal Magistrates Court.[76]

Public Interest Determinations

3.44 The Privacy Commissioner has the power to make Public Interest Determinations (PIDs) and Temporary Public Interest Determinations (TPIDs) that exempt certain acts and practices from the operation of the Act, where they would otherwise be a breach of the IPPs or NPPs.[77] The Commissioner may issue a PID where he or she is satisfied that the public interest in an agency or organisation doing an act or engaging in a practice substantially outweighs the public interest in adhering to the IPPs or NPPs. The Privacy Commissioner may make a TPID, in limited circumstances, where an application for a PID contains matters of an urgent nature.

3.45 The Privacy Commissioner has made nine PIDs to date. PIDs and TPIDs are disallowable instruments under the *Legislative Instruments Act 2003* (Cth). They must be tabled in the Australian Parliament and are then subject to disallowance.[78]

---

71 *Privacy Act 1988* (Cth) s 29.
72 Ibid pt V.
73 Ibid s 44.
74 Ibid s 45.
75 Ibid s 52.
76 Ibid s 55A.
77 Ibid ss 72, 80A and 80B.
78 Ibid ss 80 and 80C. These provisions both refer to s 46A of the *Acts Interpretation Act 1901* (Cth). That provision has been repealed. Section 6(d)(i) of the *Legislative Instruments Act 2003* (Cth) provides that instruments declared to be disallowable instruments for the purposes of section 46A of the *Acts*

Privacy Advisory Committee

3.46 The *Privacy Act* provides for the establishment of a Privacy Advisory Committee made up of the Privacy Commissioner and not more than six other members.[79] The Act requires that members of the Advisory Committee have a range of expertise, for example, in industry or public administration, the trade union movement, electronic data processing, social welfare and civil liberties.[80]

3.47 The Advisory Committee is intended to provide high level strategic advice to the Privacy Commissioner and, subject to any direction by the Commissioner, to engage in community education and consultation.[81]

Privacy regulations

3.48 Section 100 of the *Privacy Act* provides in part that:

> The Governor-General may make regulations, not inconsistent with this Act, prescribing matters:
>
> (a) required or permitted by this Act to be prescribed; or
>
> (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

3.49 Various other provisions in the Act also provide for the making of regulations. Section 6(5C), for example, states that the regulations may provide that businesses or undertakings of a specified kind are not credit reporting businesses within the meaning of the Act. Section 6E provides that the regulations may prescribe certain small business operators to be organisations for the purposes of the Act. Section 6F provides that the regulations may prescribe certain state and territory authorities and instrumentalities to be organisations for the purposes of the Act.

3.50 In Chapter 50, the ALRC proposes that the provisions dealing with credit reporting be promulgated as regulations under the *Privacy Act*.[82] In Chapter 56, the ALRC proposes that the provisions dealing specifically with the handling of health information be promulgated as regulations under the Act. Both these sets of regulations

---

Interpretation Act should be deemed legislative instruments for the purposes of the *Legislative Instruments Act*.

79 Ibid s 82. The Privacy Advisory Committee is discussed further in Ch 43.

80 The current members of the Advisory Committee are Peter Coroneos, Chief Executive Officer, Internet Industry Association; Associate Professor John M O'Brien, School of Organisation and Management, University of New South Wales; Suzanne Pigdon, former Privacy and Customer Advocacy Manager, Coles Myer Group; Dr William Pring, Director of Consultation-Liaison, Psychiatry Services, Box Hill Hospital; Joan Sheedy, Assistant Secretary, Information Law Branch, Attorney-General's Department; and Robin Banks, Chief Executive Officer, Public Interest Advocacy Centre Ltd and Director, Public Interest Law Clearing House Inc.

81 *Privacy Act 1988* (Cth) s 83.

82 Proposal 50–1.

are intended to modify the operation of the proposed Unified Privacy Principles (UPPs)—discussed in detail in Part D—in relation to credit information and health information respectively. As discussed in those chapters, the regulations need to be able to impose more *or* less stringent requirements than provided for in the UPPs.

3.51 The ALRC's view is that such modifications can be consistent with the *Privacy Act*, even where they impose less stringent requirements on agencies and organisations. It may be necessary to modify the operation of the UPPs in this way in order to achieve an appropriate balance between the public interest in protecting the privacy of individuals with other public interests, such as allowing important public health research to proceed. This is consistent with the proposed objects of the *Privacy Act* discussed further below. The ALRC is of the view that the Act should make clear that the regulations may modify the operation of the UPPs to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.

Proposal 3–1 The *Privacy Act* should provide for the making of regulations that modify the operation of the proposed Unified Privacy Principles (UPPs) to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.

The structure of the Act

3.52 Because the *Privacy Act* has been substantially amended on a number of occasions, the numbering and the structure of the Act have become confusing and difficult to navigate. For example, while the IPPs are found in s 14 of the Act, the NPPs are found in Schedule 3. In addition, the Act refers to legislation such as the *Conciliation and Arbitration Act 1904* (Cth) and provisions such as s 46A of the *Acts Interpretation Act 1901* (Cth) that have been repealed and replaced.

3.53 As discussed above, and in Parts D and E of this Discussion Paper, exemptions and exceptions are found throughout the Act and, in some cases, in other pieces of legislation. This can make it difficult to ascertain whether the *Privacy Act* covers a particular agency or organisation and, if so, to what extent. In addition, the drafting of some exemptions, such as exempt acts and practices in s 7, is complex and difficult to understand.

Submissions and consultations

3.54 A significant number of stakeholders commented on the problems caused by the complex structure of the *Privacy Act* and expressed support for some consolidation and

restructuring.[83] Electronic Frontiers Australia expressed the view that the Act was 'complex, confusing and unwieldy' and that this was leading to misapplication of the provisions.[84] The Centre for Law and Genetics agreed that the Act has become difficult to work with:

> We would strongly support the redrafting of the legislation to achieve a greater degree of simplicity and clarity. Nevertheless, the original flow from collection through to release arose from the OECD Guidelines and this remains a defensible template.[85]

3.55 The Office of the Information Commissioner Northern Territory was of the view that the *Privacy Act* had 'lost its way' and should be redrafted, using plain English, and restructured, including grouping exemptions together.[86] A number of commentators have also been critical of the Act's complexity.[87]

ALRC's view

3.56 In the ALRC's view, such complexity seems undesirable in legislation intended to protect individuals' personal information. An individual is unlikely to be able to take action to protect his or her rights if it is difficult to ascertain what acts and practices of agencies and organisations are covered by the legislation.

3.57 In Chapter 15, the ALRC proposes a single set of UPPs applying both to agencies and organisations.[88] This change will resolve much of the complexity in the current provisions. In Chapter 30 the ALRC proposes that the exemptions in the *Privacy Act* should be clarified and located together.[89] Amending the *Privacy Act* in line with these proposals would provide an excellent opportunity to restructure the Act entirely to achieve greater logical consistency, simplicity and clarity.

---

83 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Law Institute of Victoria, *Submission PR 200*, 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; AAMI, *Submission PR 147*, 29 January 2007; Confidential, *Submission PR 143*, 24 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007; Tasmanian Ombudsman, *Consultation PC 158*, Hobart, 30 March 2007.

84 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

85 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

86 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

87 R Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (1989) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html> at 30 July 2007, [6.1]; T Dixon, 'Preparing for the New Privacy Legislation' (Paper presented at Australia's New Privacy Legislation, Baker & McKenzie Cyberspace Law and Policy Centre CLE Conference, Sydney, 24–25 May 2001).

88 Proposal 15–2.

89 Proposal 30–1.

Proposal 3–2 The *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity. For example, the Information Privacy Principles and the National Privacy Principles should be consolidated into a set of UPPs; the exemptions should be clarified and grouped together in a separate part of the Act; and the Act should be restructured and renumbered.

The name of the Act

3.58 The *Privacy Act* is essentially limited in its scope to the protection of personal information. It does not regulate other elements of the right to privacy, for example, the right to be free from arbitrary or unlawful interference with one's home or family life. The Privacy Commissioner, Karen Curtis, noted in evidence to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry):

> I think we should all remember that, while our Privacy Act is about the protection of personal information or sensitive information, it is really about data protection. It is not about privacy in the broader sense of bodily privacy or privacy in other areas. I think 'privacy' is often seen as a catch-all and so our Privacy Act does not address all aspects of territorial privacy or bodily privacy.[90]

3.59 The Australian Government is not alone in using this nomenclature for legislation that protects personal information. Both Canada and New Zealand have a Privacy Act. The Canadian *Privacy Act 1985* regulates the handling of personal information by the public sector. The New Zealand *Privacy Act 1993* regulates the handling of personal information in both the public and the private sector.

3.60 Names given to similar legislation in a number of other jurisdictions, however, indicate more accurately the scope of the legislation; for example:

- *Privacy and Personal Information Protection Act 1998* (NSW);
- *Information Privacy Act 2000* (Vic);
- *Personal Information Protection Act 2004* (Tas);
- *Information Act 2002* (NT);
- *Data Protection Act 1998* (United Kingdom);

90 Commonwealth, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 51 (K Curtis—Privacy Commissioner).

- *Personal Information Protection and Electronic Documents Act 2000* (Canada).[91]

3.61 Nomenclature in the legislative context is important because accurate descriptive names provide a snapshot of the content of the legislation. Names may also serve political purposes, for example, assisting the passage of a Bill through Parliament, and may act to publicise the legislation locally and internationally.[92] Names that do not describe accurately the scope of legislation may mislead the public into believing that a law covers particular areas that, in fact, it does not.

Submissions and consultations

3.62 A number of submissions expressed support for the current name of the *Privacy Act*.[93] The OPC noted that the functions of the Privacy Commissioner set out in s 27 of the Act are wider than the protection of personal information. They include education to promote the protection of individual privacy[94] and recommendations to the Attorney-General on the need for legislative or administrative action in the interests of privacy.[95]

> Moreover, the Office observes that information privacy can intersect with other categories of privacy. For example, location detection technologies, which collect information about an individual's whereabouts, might be considered to cut across both information and physical privacy. In the view of the Office, the Privacy Act should therefore continue to be an instrument that can effectively respond to these broader privacy issues.[96]

3.63 The OPC expressed the view in its submission that the Act should be renamed the Australian Privacy Act to differentiate it more clearly from privacy legislation in other jurisdictions.

3.64 On the other hand, there was considerable support for renaming the legislation to focus more expressly on the protection of personal information. Options suggested included:

- Information Privacy Act;[97]

---

91 The *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) regulates the handling of personal information by the private sector.

92 M Whisner, 'What's in a Statute Name?' (2005) 97 *Law Library Journal* 169, 183.

93 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

94 *Privacy Act 1988* (Cth) s 27(1)(m).

95 Ibid s 27(1)(r).

96 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

97 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Law Institute of Victoria, *Submission PR 200,* 21 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law

- Personal Information Privacy Act;[98]
- Personal Information Regulation Act;[99]
- Protection of Personal Information Act;[100]
- Privacy and Information Protection Act;[101]
- Data Protection Act;[102] and
- Privacy and Data Protection Act.[103]

3.65 The Australian Privacy Foundation did not support the use of the name Data Protection Act because it might imply that the legislation was limited to computerised information or was only concerned about security.[104]

3.66 The point was made in one submission that, in considering the name of the Act, it is necessary to consider whether the Act is to be extended to include a wider cause of action for invasion of privacy.[105]

ALRC's view

3.67 In Chapter 43, the ALRC proposes that the Office of the Privacy Commissioner be renamed the Australian Privacy Commission. One option would be to rename the Act the Australian Privacy Commission Act. The ALRC's view, however, is that the name of the Act should not focus on the establishment of the Commission, but on the substantive role of the legislation, that is, to protect privacy.

3.68 The ALRC does not agree that the Act should be renamed the Australian Privacy Act as suggested by the OPC. 'Australian' is often included in the title of legislation at the national level where it forms part of the name of the organisation established by the legislation, for example, *Australian Law Reform Commission Act 1996* (Cth). Where this is not the case, the relevant jurisdiction is traditionally indicated by a bracketed abbreviation following the name of legislation: *Privacy Act*

---

and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; L Bygrave, *Submission PR 92*, 15 January 2007.

98 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

99 Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

100 Confidential, *Submission PR 143*, 24 January 2007.

101 National Association for Information Destruction, *Submission PR 133*, 19 January 2007.

102 National Association for the Visual Arts, *Submission PR 151*, 30 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

103 W Caelli, *Submission PR 99*, 15 January 2007.

104 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

105 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

1988 (Cth). This avoids the need to include the word 'Australian' in the name of all federal legislation.

3.69 In Chapter 5, the ALRC proposes the establishment of a statutory cause of action for invasion of privacy. Proposal 5–1 suggests that this statutory cause of action be included in the *Privacy Act*. The statutory cause of action would arise in a range of situations, including where there has been an interference with an individual's home or family life, an individual has been subjected to unauthorised surveillance, or an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed. If the *Privacy Act* is amended in accordance with this proposal, the ALRC is of the view that the name of the Act should remain the same.

3.70 If the *Privacy Act* is not amended to include a statutory cause of action, the ALRC has formed the preliminary view that the Act should be renamed the *Privacy and Personal Information Act*. The ALRC is of the view that the current name of the *Privacy Act* does not accurately reflect the main focus of the legislation and has the potential to cause confusion. This is a particular problem with a term such as 'privacy', which potentially covers a number of areas and is in general use in the community in relation to matters that are not covered by the *Privacy Act*. The proposed name more clearly reflects the main focus of the Act, that is, the privacy of personal information, while at the same time being wide enough to encompass the fact that the Privacy Commissioner has a number of functions that do not relate to personal information.

Proposal 3–3 If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, the name of the Act should remain the same. If the Act is not amended in this way, however, the *Privacy Act* should be renamed the *Privacy and Personal Information Act*.

The objects of the Act

3.71 According to the former Privacy Commissioner, Malcolm Crompton:

> This light touch approach has manifested itself in the form of a principles based, rather than a prescriptive approach, to changing behaviour for the private sector at large … Although there may be good reasons for a less prescriptive approach, this kind of legislative regime leaves regulators with substantial uncertainty and ambiguity as they go about implementing and enforcing the law especially in the early phases.[106]

106 M Crompton, *'Light Touch' or 'Soft Touch'—Reflections of a Regulator Implementing a New Privacy Regime* (2004).

3.72 An objects clause is a provision—often located at the beginning of a piece of legislation—that outlines the underlying purposes of the legislation and can be used to resolve uncertainty and ambiguity. Objects clauses have been described as a 'modern day variant on the use of a preamble to indicate the intended purpose of legislation'.[107] The Office of Parliamentary Counsel, which is responsible for drafting Australian Government legislation, has noted that:

> One of the most valuable aids to detailed understanding of a complex set of provisions is a general understanding of the purpose, structure and direction of the provisions … Some objects provisions give a general understanding of the purpose of the legislation … Other objects provisions set out general aims or principles that help the reader to interpret the detailed provisions of the legislation.[108]

3.73 Objects clauses may assist the courts and others in the interpretation of legislation.[109] Section 15AA of the *Acts Interpretation Act 1901* (Cth) states that:

> In the interpretation of a provision of an Act, a construction that would promote the purpose or object underlying the Act (whether that purpose or object is expressly stated in the Act or not) shall be preferred to a construction that would not promote that purpose or object.

3.74 The interpretation Acts of the states and territories contain similar or identical provisions.[110] Cole JA of the New South Wales Court of Appeal has made clear that

> whilst regard may be had to an objects clause to resolve uncertainty or ambiguity, the objects clause does not control clear statutory language, or command a particular outcome of exercise of discretionary power.[111]

International instruments

3.75 The *Privacy Act* does not include a section setting out the objects of the legislation. The Act does include a Preamble that indicates that the legislation is intended to give effect to Australia's obligations in relation to privacy under the ICCPR and to implement the OECD Guidelines. The Preface to the OECD Guidelines states in part that

> although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.[112]

---

107 D Pearce and R Geddes, *Statutory Interpretation in Australia* (6th ed, 2006), 154.

108 Office of Parliamentary Counsel, *Working with the Office of Parliamentary Counsel: A Guide for Clients* (2nd ed, 2002), [116]–[117].

109 See, eg, *Tickner v Bropho* (1993) 114 ALR 409.

110 *Interpretation Act 1987* (NSW) s 33; *Interpretation of Legislation Act 1984* (Vic) s 35(a); *Acts Interpretation Act 1954* (Qld) s 14A; *Interpretation Act 1984* (WA) s 18; *Acts Interpretation Act 1915* (SA) s 22; *Acts Interpretation Act 1931* (Tas) s 8A; *Interpretation Act 1978* (NT) s 62A.

111 *Minister for Urban Affairs and Planning v Rosemount Estates Pty Ltd* (1996) 91 LGERA 31, 78.

112 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Preface.

3.76 Other international instruments also set out their aims and objects. Article 1 of the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* (EU Directive), states that:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.[113]

3.77 The Preamble to the Asia-Pacific Economic Cooperation (APEC) Privacy Framework states that:

> Finally, this Framework on information privacy protection was developed in recognition of the importance of:
>
> - Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
> - Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;
> - Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
> - Enabling enforcement agencies to fulfill their mandate to protect information privacy; and
> - Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.[114]

Federal legislation

3.78 Although the *Privacy Act* does not include an objects clause, s 29 of the Act requires the Privacy Commissioner to have regard to a number of matters in performing his or her functions. These include the protection of important human rights and social interests that compete with privacy such as the general desirability of a free flow of information, through the media and otherwise, and the right of

---

113 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 1 Objects of the Directive.

114 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Preamble.

government and business to achieve their objectives in an efficient way.[115] The Commissioner is also required to take into account Australia's international obligations, including those concerning the international technology of communications and developing general international guidelines relevant to the better protection of individual privacy.[116] The Commissioner must also ensure that his or her recommendations and guidelines are, within the limitations of the powers of the Commonwealth, capable of acceptance, adaptation and extension throughout Australia.[117]

3.79 Section 3 of the *Privacy Amendment (Private Sector) Act* states that the main objects of that Act are:

> (a) to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations; and
>
> (b) to do so in a way that:
>
> (i) meets international concerns and Australia's international obligations relating to privacy; and
>
> (ii) recognises individuals' interests in protecting their privacy; and
>
> (iii) recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently.

3.80 A number of other federal Acts in the field of human rights—including the *Sex Discrimination Act 1984* (Cth), the *Disability Discrimination Act 1992* (Cth) and the *Age Discrimination Act 2004* (Cth)—include an objects clause. Recent federal Acts containing an objects clause include the *Future Fund Act 2006* (Cth), the *Energy Efficiency Opportunities Act 2006* (Cth) and the *Law Enforcement Integrity Commissioner Act 2006* (Cth).

State and territory privacy legislation

3.81 The *Information Privacy Act 2000* (Vic),[118] the *Information Act 2002* (NT)[119] and the Information Privacy Bill (WA)[120] expressly set out their objects. The *Privacy and Personal Information Protection Act 1998* (NSW) and the *Personal Information Protection Act 2004* (Tas), however, do not include an objects clause.

---

115 *Privacy Act 1988* (Cth) s 29(a).
116 Ibid s 29(b).
117 Ibid s 29(c).
118 *Information Privacy Act 2000* (Vic) s 5.
119 *Information Act 2002* (NT) s 3.
120 Information Privacy Bill 2007 (WA) cl 3.

3.82 Section 5 of the Victorian *Information Privacy Act* provides that the objects of that Act are:

> (a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
>
> (b) to promote awareness of responsible personal information handling practices in the public sector;
>
> (c) to promote the responsible and transparent handling of personal information in the public sector.

Submissions and consultations

3.83 There was significant support for amending the *Privacy Act* to include an objects clause.[121] The Office of the Information Commissioner Northern Territory stated that:

> I consider that the impact of the privacy principles could be significantly enhanced by a brief statement of the overarching objects to guide those who must interpret and implement them. This could either appear as an introductory statement to the principles or as an objects clause at the start of the Act.[122]

3.84 The National Health and Medical Research Council (NHMRC) suggested that an objects clause would assist health service providers, researchers and others to understand the overall purpose, structure and direction of the legislation and, on that basis, better interpret and apply the legislation.[123]

3.85 Stakeholders suggested that the objects of the *Privacy Act* might include:

- to balance the public interest in protecting individual privacy with other public interests;[124]

---

121 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Law Institute of Victoria, *Submission PR 200*, 21 February 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Australian Federal Police, *Submission PR 186*, 9 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; National Association for Information Destruction, *Submission PR 133*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007; National Health and Medical Research Council, *Submission PR 114*, 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007.

122 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

123 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

124 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Government of South Australia, *Submission PR 187*, 12 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; AAMI, *Submission PR 147*, 29 January 2007.

- to secure the right of individuals to control the dissemination of information about their own lives;[125]
- to promote the responsible and transparent handling of personal information;[126]
- to protect the information privacy of individuals while authorising appropriate uses of their personal information;[127]
- to achieve national consistency;[128] and
- the matters set out in s 29 of the *Privacy Act*, as discussed above.[129]

ALRC's view

3.86 The ALRC's view is that the *Privacy Act* would benefit from the inclusion of an objects clause setting out the purpose and aims of the legislation. This is particularly important in principles-based legislation because principles require constant interpretation and application to particular contexts and an objects clause provides a reference framework to assist with this.

3.87 Some of the matters set out in s 29 of the *Privacy Act* for consideration by the Privacy Commissioner in carrying out his or her functions would sit more appropriately in an objects clause. These matters are relevant to the interpretation and application of the Act by all stakeholders, not only the Privacy Commissioner.

3.88 The ALRC proposes, therefore, that the objects clause include the following elements. The clause should state that one of the objects of the Act is to implement Australia's obligations at international law in relation to privacy. This provides a pointer to relevant international instruments and jurisprudence that may assist in interpreting and applying the legislation. The clause should also state that the Act is intended to promote the protection of individual privacy. The right to privacy is one of a number of fundamental human rights set out in the ICCPR and other international instruments and, while the right is not absolute, one of the objects of the *Privacy Act* should be to promote protection of that right.

3.89 Chapter 1 discusses how the right to privacy competes, collides and coexists with other rights and interests, such as freedom of expression. The objects clause should expressly recognise these tensions and make clear that the Act is intended to provide a framework within which agencies and organisations must balance the public interest in protecting the privacy of individuals with other public interests. Although

---

125 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105*, 16 January 2007.
126 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.
127 Australian Federal Police, *Submission PR 186*, 9 February 2007.
128 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007.
129 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007.

the right to privacy is an individual right, there is a strong public interest in protecting that right. For example, it is essential that health consumers are confident that their health information will be handled appropriately or they may resist sharing that information with health service providers. This has the potential to have a negative impact on the health of the individual and is also an undesirable public policy outcome, with the potential to impact on the health of the community as a whole.

3.90 Chapter 5 proposes the *Privacy Act* be amended to include a statutory cause of action for invasion of privacy. The objects clause should reflect that the Act and the statutory cause of action are not limited to the protection of personal information but are intended to protect a wider set of interests that individuals have in the personal sphere free from the interference of others.

3.91 The objects clause should also make clear that the Act and, in particular, the UPPs are intended to promote the responsible and transparent handling of personal information by agencies and organisations. This will help to ensure respect for the right to privacy while, at the same time, facilitating the growth and development of electronic commerce, nationally and internationally.

3.92 Finally, the objects clause should make clear that the Act is intended to provide the basis for nationally consistent regulation in the area of privacy. Chapter 4 sets out the ALRC's proposals to achieve greater national consistency.

Proposal 3–4 The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be to:

(a) implement Australia's obligations at international law in relation to privacy;

(b) promote the protection of individual privacy;

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;

(d) establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy; and

(g) provide the basis for nationally consistent regulation of privacy.

Some important definitions

3.93 Part II of the *Privacy Act* sets out a number of important definitions. While these will be discussed in detail, where relevant, throughout this Discussion Paper, some core definitions are discussed below.

Personal information

3.94 Central to the regime established by the *Privacy Act* is the definition of 'personal information'. This is because the privacy principles only apply to personal information. The current definition of 'personal information' is the same as the definition found in the original 1988 Act:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[130]

3.95 A number of submissions to the Senate Committee privacy inquiry suggested that the definition of 'personal information' in the Act needed to be updated to deal with new technologies and new methods of collecting information.[131] Research done on behalf of the Consultative Committee of the Council of Europe Convention has also highlighted that new technology makes it possible to process data relating to individuals—and to develop profiles of those individuals—that are not linked to their legal identity such as their name and address.[132]

3.96 Both the OPC and the Senate Committee recommended that the ALRC, in its review of the *Privacy Act*, examine the definition of 'personal information' and any amendments to the definition that may be needed to reflect technological advances and international developments in privacy law.[133]

---

130 *Privacy Act 1988* (Cth) s 6(1).

131 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19]–[3.24]; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005; Centre for Law and Genetics, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 February 2005.

132 Y Poullet, *Report on the Application of Data Protection Principles to the Worldwide Telecommunications Networks* (2004) Council of Europe, 33.

133 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 7.15; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 69.

International instruments

3.97 The OECD Guidelines[134] and the Council of Europe Convention[135] define 'personal data' as 'any information relating to an identified or identifiable individual'. The EU Directive defines 'personal data' as 'any information relating to an identified or identifiable natural person' and goes on to say that an identifiable person is

> one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[136]

3.98 The APEC Privacy Framework defines 'personal information' as 'any information about an identified or identifiable individual.' The Framework goes on to state that this includes information that can be used to identify an individual, as well as information that would not meet this criteria alone, but when put together with other information would identify an individual.[137]

Other jurisdictions

3.99 A 2004 report on the meaning of 'personal data' prepared for the United Kingdom Information Commissioner examined the definition and application of the term in the privacy legislation of 18 countries. The report found that there is 'no one uncontested and coherent definition' of 'personal data'.[138]

3.100 The *Data Protection Act 1998* (UK) states that 'personal data' means:

> data which relate to a living individual who can be identified
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[139]

---

134 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), art 1.

135 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985), art 2.

136 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 2.

137 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [9].

138 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 8.

139 *Data Protection Act 1998* (UK) s 1(1).

3.101 Both the Canadian *Personal Information Protection and Electronic Documents Act 2000*[140] and the New Zealand *Privacy Act 1993*[141] simply define 'personal information' as 'information about an identifiable individual'.

3.102 The Information Privacy Bill 2007 (WA) defines personal information in part as follows:

> Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead—
>
> (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or
>
> (b) who can be identified by reference to an identifier or an identifying particular such as a fingerprint, retina print or body sample.[142]

Submissions and consultations

3.103 A number of submissions expressed support for the existing definition.[143] The Australian Bankers' Association stated that changing key definitions in the *Privacy Act* would come at some cost to industry and should only be done if a clear case for change is made out.[144] DLA Phillips Fox noted in its submission that the current definition is broad enough to capture information in any medium and sufficiently flexible to allow for future technological developments.[145]

3.104 There was support for keeping the definition technologically neutral.[146] Technological neutrality supports technological change. The OPC noted that:

> The definition of personal information is contingent on context for its application. In the view of the Office, this is one of the strengths of the definition, allowing it to respond to change and technological advance. In order to alleviate any confusion generated by the flexibility of the term, the Office intends to issue further guidance material.[147]

3.105 A number of stakeholders expressed support for the definition of 'personal information' included in the EU Directive.[148]

---

140 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 2(1).
141 *Privacy Act 1993* (NZ) s 1.
142 Information Privacy Bill 2007 (WA) cl 6.
143 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; AXA, *Submission PR 119*, 15 January 2007; Telstra, *Submission PR 185*, 9 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; AXA, *Submission PR 119*, 15 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007.
144 Australian Bankers' Association Inc, *Submission PR 259*, 19 March 2007; Telstra, *Submission PR 185*, 9 February 2007.
145 DLA Phillips Fox, *Submission PR 111*, 15 January 2007.
146 AAMI, *Submission PR 147*, 29 January 2007; DLA Phillips Fox, *Submission PR 111*, 15 January 2007.
147 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
148 AAMI, *Submission PR 147*, 29 January 2007; Australia Post, *Submission PR 78*, 10 January 2007.

About an individual

3.106 The current definition in the *Privacy Act* states that information must be 'about an individual'. The APEC Privacy Framework also requires that information be 'about' an individual. The OECD Guidelines, the Council of Europe Convention and the EU Directive require that information 'relate to' an individual.

3.107 The 2004 report prepared for the United Kingdom Information Commissioner, however, notes that not all data that relate to an individual should fall within the definition of 'personal information'. To hold that all information that could affect or be linked to an individual is 'personal information' 'runs the risk of making all data personal data'. The limiting factor is that the information must relate to an identifiable individual: the information must either identify the individual or be able to be linked to information that can identify the individual. The report defines this kind of information as being 'about' the individual.[149]

3.108 Veda Advantage noted that if the definition of 'personal information' were expanded to include information that 'referred to' or 'related to' an individual, it would make large scale data studies—where privacy is protected by de-identifying information or encrypting significant elements—impossible.[150]

3.109 One other issue that arose in submissions and consultations was whether business or commercial information was 'about' an individual, for example, information on the number and type of prescriptions issued by a particular doctor, where patient identifiers have been removed. It was suggested that this kind of information should not be protected by the *Privacy Act* as it relates to the individual doctor's business practices, rather than his or her personal affairs.[151] The Article 29 Data Protection Working Party, however, has stated that:

> Drug prescription information … whether in the form of an individual prescription or in the form of patterns discerned from a number of prescriptions, can be considered as personal data about the physician who prescribes this drug, even if the patient is anonymous.[152]

3.110 The OPC has also stated that, if an individual's identity can be determined from business information, the information is personal information for the purposes of the

149 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 11.

150 Veda Advantage, *Submission PR 163*, 31 January 2007.

151 Australian Health Insurance Association, *Submission PR 161*, 31 January 2007; IMS Health Asia, *Consultation PC 124*, Sydney, 8 March 2007.

152 European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP136 (2007).

Privacy Act.[153] The Australian Government noted in its response to the recommendations of the *Taskforce on Reducing the Regulatory Burden on Business* that the publication of detailed information on the charging practices and performance of health service providers is likely to have industry wide implications and any proposed reform would need to take these implications into account.[154]

3.111 While the *Privacy Act* would not stand in the way of this kind of regulatory reform, in the absence of such reform the *Privacy Act* will apply to such information. The extent to which business or commercial information is 'about' an individual and, therefore, constitutes 'personal information' is also considered in Chapter 50 in relation to credit reporting and Chapter 57 in relation to health service providers.

Whose identity is apparent, or can reasonably be ascertained

3.112 In 2002, the then Privacy Commissioner, Malcolm Crompton, stated that 'Identity and anonymity are not binary opposites, but rather different ends of the same spectrum and there are many shades of grey between them'.[155]

> An important distinction needs to be made between identity and identification. Identity is a complex, multifaceted notion. Each of us has a range of different identities defined through relations with others, position, status, actions, behaviours, characteristics, attitudes and the circumstances of the moment …
>
> Identification is the action of being identified, of linking specific information with a particular person. An individual's identity has a degree of fluidity and is likely to change over time. The extensive linking of different information about an individual may restrict or limit this fluidity …
>
> Identification can potentially relate a wide range of elements of an individual's identity. In practice, identifying an individual generally involves focusing on those things that distinguish that individual from others including, legal name, date of birth, location or address and symbolic identifiers such as a drivers license number.[156]

3.113 A number of submissions to the Inquiry expressed concern that, with the advent of the internet and other technologies—such as location based services including mobile phones and the Global Positioning System (GPS)—it is possible to build profiles of individuals using identifiers such as mobile phone numbers.[157] The 2004 report prepared for the United Kingdom Information Commissioner notes that:

> 'Identification' can potentially refer to at least two very different concepts. The first could be termed 'handshake' identification. This concept of identification requires

---

153 Office of the Privacy Commissioner, *Frequently Asked Questions: When is Business Information Covered by the Privacy Act?* <www.privacy.gov.au/faqs/bf/q8.html> at 30 July 2007.

154 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 5–6.

155 M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

156 Ibid.

157 AAMI, *Submission PR 147*, 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

> that the individual concerned can actually be physically located, in order to enable a 'handshake' to take place. The second could be termed 'isolate and affect' identification. This holds that no such physical location is required; instead; identification is achieved if an individual can be effectively isolated from others and deliberately targeted in some way. Such identification may be regularly realised within electronic environments.[158]

3.114 The report provides the following example:

> An example may be provided by those individuals who 'date' online in chat rooms while concealing details of their 'real' identities or physical locations. While incapable of locating each other for the purposes of a 'handshake' they may nevertheless be able to consistently and reliably 'identify' and 'affect' each other in their virtual environment.[159]

3.115 However, the report notes that:

> Under the 'handshake' concept of identification, it would be difficult to see how the individual identified could be anything other than a living, natural person. If the 'isolate and affect' concept of identification is employed, then this could *potentially* apply to legal persons. In fact, taken to its extreme, such a concept of identification could legitimise the protection of personal data belonging to imaginary persons.[160]

3.116 Electronic Frontiers Australia has suggested including the following in the definition of 'personal information':

> Any information which enables interactions with an individual on a personalised basis, or enables tracking or monitoring of an individual's activities and/or communication patterns, or enables an individual to be contacted.[161]

3.117 The Australian Privacy Foundation suggested that the definition of personal information should include telephone numbers, email or IP addresses and information stored with an identifier code or label:

> Personal information needs to be defined as any information from which an individual can be identified, whether from the information itself or by reference to other information in the possession of, or readily accessible to, the data user.[162]

3.118 Professor William Caelli noted that, in the context of internet based information services,

---

158 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 127.

159 Ibid, 127.

160 Ibid, 128.

161 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

162 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

> the use of pseudonyms, aliases and the like appears common, or even total, in this environment. Users maintain their privacy through protection of an 'association', ie, exposure of the relationship between the assumed 'internet' identity and 'real' identity.[163]

3.119 He notes that, in order to ensure an individual's privacy, it is necessary to protect this association.

3.120 The United Kingdom Information Commissioner has issued detailed legal guidelines on the *Data Protection Act 1998* (UK) including in relation to the meaning of 'personal data'. Under the *Data Protection Act*, the individual must be capable of being identified from data in the possession of the data controller, or from those data and other information in the possession of, or likely to come into the possession of, the data controller:

> The Commissioner recognises that an individual may be 'identified' without necessarily knowing the name and address of that particular individual.
>
> The Commissioner's view is that it is sufficient if the data are capable of being processed by the data controller to enable the data controller to distinguish the data subject from any other individual. This would be the case if a data subject could be treated differently from other individuals …
>
> If the information about a particular web user is built up over a period of time, perhaps through the use of tracking technology, with the intention that it may later be linked to a name and address, that information is personal data. Information may be compiled about a particular web user, but there might not be any intention of linking it to a name and address or e-mail address. There might merely be an intention to target that particular user with advertising, or to offer discounts when they re-visit a particular web site, on the basis of the profile built up, without any ability to locate that user in the physical world. The Commissioner takes the view that such information is, nevertheless, personal data. In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others.[164]

3.121 DLA Phillips Fox suggested in its submission that:

> The current definition … does not require the identification of an individual by reference to the individual's legal identifiers, but rather that their identity can 'be reasonably ascertained'. This is sufficiently broad to ensure that advances in data processing and storage methods will not result in information capable of being associated with an individual falling outside the ambit of the Privacy Act.[165]

3.122 The OPC expressed the following view in its submission:

> The definition of personal information provides latitude for the Office to take into consideration contextual factors when determining if information should be subject to

---

163 W Caelli, *Submission PR 99*, 15 January 2007.

164 United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 11.

165 DLA Phillips Fox, *Submission PR 111*, 15 January 2007.

> the *Privacy Act*. These contextual factors go to determining whether an individual's identity is 'readily ascertainable'.
>
> The Office recognises the challenges posed by the development of new technologies and processes, particularly in the field of data-matching, that have the potential to create identified information from data sources containing previously anonymous data. However, the definition of personal information leaves open the flexibility to consider the degree to which an organisation is able to 'reasonably ascertain' someone's identity, including by the use of such technologies.[166]

3.123 The OPC has expressed the view that this may depend on the resources available to an organisation to re-identify the information.[167] The OPC has suggested that it issue further guidance on what is 'personal information' taking into account the fact that in the current environment it is more difficult to assume that information about people cannot be connected.[168]

Ability to contact

3.124 A number of submissions supported expanding the definition of 'personal information' to include information that allows an individual to be contacted. The Australian Privacy Foundation suggested that the definition should include information sufficient to allow communications with an individual whether or not it is sufficient to allow the individual to be identified.[169]

3.125 On the other hand, Australia Post expressed the following concern:

> The Corporation further submits that any move to extend the definition of personal information to include 'contact information' or otherwise prevent the ability of a business to contact an unidentifiable individual, would be inconsistent with the policy objectives of Privacy Act.[170]

3.126 The OPC has made clear that a business can use personal information taken from public sources—such as the phone book—to contact potential customers. Thus, even if contact information were 'personal information', businesses could use the information to contact individuals. The obligations imposed by the *Privacy Act* in these circumstances would be to:

---

166 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

167 Office of the Privacy Commissioner, 'De-identification of Personal Information', (Paper presented at Privacy Contact Officers Network Meeting, Canberra, 26 November 2004).

168 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 72.

169 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

170 Australia Post, *Submission PR 78*, 10 January 2007.

- tell potential customers the business' name and how to contact it, why the information has been collected, to whom the business usually discloses such information and how the customer can get access to the information (NPP 1.5);

- only use the information for the purpose it was collected, that is to approach the customer, or for a related purpose that the potential customer would expect (NPP 2.1(a));

- do what is reasonable to make sure the information is correct and to delete or correct information that it finds is not correct (NPP 3);

- keep the information reasonably secure (NPP 4);

- have a privacy policy (NPP 5); and

- give the potential customer access to the information on request and correct any errors the customer points out (NPP 6).[171]

ALRC's view

3.127 The current definition of 'personal information' contains the following elements:

- information or an opinion;

- including information or an opinion forming part of a database;

- whether true or not;

- whether recorded in a material form or not;

- about an individual;

- whose identity is apparent from the information or opinion; or

- whose identity can reasonably be ascertained from the information or opinion.[172]

Elements requiring no change

3.128 The ALRC proposes that the following elements of the definition should remain unchanged: information or an opinion, whether true or not, and whether recorded in a

171 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001).
172 *Privacy Act 1988* (Cth) s 6(1).

material form or not. The ALRC did not receive any submissions indicating that these elements of the definition were problematic.

3.129 The ALRC is also of the view that 'about' an individual remains appropriate and effective. The ALRC notes that, although a number of international instruments use the term 'relates to', the *Privacy Act* terminology is consistent with the APEC Privacy Framework.

Forming part of a database

3.130 The ALRC is of the view that the second element of the definition—'including information or an opinion forming part of a database'—is unnecessary and should be deleted. It may have been helpful to make this clear in 1988 when the *Privacy Act* was originally passed, but in the current environment it is no longer a matter of uncertainty. In addition, the proposed definition of 'record', discussed below, expressly includes 'information stored in electronic or other forms'.

Whose identity is apparent or can reasonably be ascertained

3.131 The ALRC's view is that this element of the definition should be amended to bring it more into line with other jurisdictions and international instruments. The ALRC proposes that 'personal information' should be defined as information about 'an identified or reasonably identifiable individual'. The ALRC notes the distinction drawn by the former Privacy Commissioner between 'identity' and 'identification' and is of the view that the *Privacy Act* should apply to information about an individual who is 'identified or reasonably identifiable' rather than information about an individual whose 'identity' is apparent, or can reasonably be ascertained.

3.132 The ALRC notes the difficulties that stakeholders have with the existing definition and is of the view that using terminology that is more consistent with that used in relevant international instruments may assist. International jurisprudence and explanatory material based on the terms 'identified' and 'identifiable' will be more directly relevant. The APEC Privacy Framework, the OECD Guidelines, the Council of Europe Convention and the EU Directive use the terms 'identified' and 'identifiable'.

3.133 In the ALRC's view, the definition should include an element of reasonableness. Whether an individual can be identified or is identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds by, for example, linking the information with information held by another agency or organisation, it may be that it is not practically possible because, for example, of logistics or legislation. In these circumstances, the ALRC is of the view that individuals are not 'reasonably identifiable'.

3.134 If, however, the agency or organisation does have access to other information and is able to link that information with information it holds in such a way that individuals can be identified, the ALRC is of the view that those individuals are 'reasonably identifiable' and that the information is 'personal information' for the purposes of the *Privacy Act.* For this reason, the definition of 'personal information' should not be limited, as it currently is, to information about an individual who can be identified 'from the information'. The ALRC proposes that the Explanatory Memorandum to the amended Act make clear that an individual is 'reasonably identifiable' when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.

3.135 This issue is discussed further in Chapter 58 in relation to research, data linkage and the use of intermediaries such as 'gene trustees'. Where an independent intermediary is used to remove identifying particulars and to code information provided to researchers, the ALRC is of the view that this is an effective method of protecting privacy. Where appropriate arrangements are put in place between data custodians, intermediaries and researchers, the ALRC is of the view that the information in the hands of researchers is not 'identified or reasonably identifiable' for the purposes of the *Privacy Act*.

3.136 The ALRC notes the United Kingdom Information Commission's view that information need not be linked to a name and address in order for the individual to be 'identified' and that, where information allows an agency or organisation to distinguish an individual from any other individual, this amounts to personal information. The examples provided included the collection of information about internet users with the intention of linking that information to names and addresses; and targeting individuals with advertising without linking the information to names and addresses or making any effort to identify individuals in the physical world. The Commissioner takes the view that such information is personal information. The ALRC agrees that this information should be protected by the *Privacy Act* and would fall within the proposed definition of personal information.

3.137 The ALRC does not agree, however, that 'information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others'.[173] In the ALRC's view, this is not sufficient to amount to 'personal information'. The use of an independent intermediary to code information for release to researchers allows researchers to distinguish one individual from others and to link information about that individual, without being able to 'identify' the individual. In order for information to identify an individual, it must be possible to use the information to contact, target or affect the individual in some way. If it is not possible

173 United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 11.

to make this link with a particular individual then, in the ALRC's view, the information is not about an 'identified' or 'reasonably identifiable' individual.

3.138 Electronic Frontiers Australia has suggested that the definition of 'personal information' be amended to include information that enables interactions with an individual on a personalised basis, or enables tracking or monitoring of an individual's activities and/or communication patterns. In the ALRC's view, the proposed amended definition of 'personal information' would cover 'information that enables interactions with an individual on a personalised basis'. It would also cover information that enables 'tracking or monitoring of an individual's activities and/or communication patterns' if a link can be established to a particular individual and that individual can be contacted, targeted or affected in some way.

Ability to contact

3.139 In the ALRC's view, information that simply allows an individual to be contacted—such as a phone number, a street address or an IP address—in isolation, would not fall within the proposed definition of 'personal information'. The *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. This broader issue is discussed in Chapter 1 in relation to the meaning of 'privacy'. Contact information may become 'personal information' in certain contexts, for example, once a mobile number is linked to a particular individual or the number can reasonably be linked to a particular individual. If an agency or organisation can reasonably ascertain the identities of direct mail recipients by linking data in the address database with particular names in the same or another database, that information is 'personal information' and should be treated as such.

3.140 As information accretes around a point of contact such as a telephone number, an address, an email address or an IP address, it will become possible to link that information to a particular individual, to contact or affect that individual or to target the individual, for example, with advertising material. Once this occurs, that information becomes 'personal information' for the purposes of the *Privacy Act.*

Conclusion

3.141 The then Privacy Commissioner, Malcolm Crompton expressed the view that:

> Privacy laws need to be in the form of general principles, as information handling is highly contextual. This can create a significant margin for interpretation and implementation.[174]

174 M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

3.142 Because of this, elements of the definition of 'personal information' will continue to give rise to theoretical uncertainty. While much information will fall clearly inside or outside the definition, there will be a need for ongoing practical guidance in relation to those areas of uncertainty. The OPC has suggested that the Office issue further guidance on the meaning of 'personal information'. The ALRC agrees that such guidance will be necessary to indicate how the definition operates in specific contexts. In particular, the ALRC proposes that the OPC issue guidance on the meaning of 'identified or reasonably identifiable'.

Proposal 3–5 (a) The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

(b) The Explanatory Memorandum of the amending legislation should make clear that an individual is 'reasonably identifiable' when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.

(c) The Office of the Privacy Commissioner should provide guidance on the meaning of 'identified or reasonably identifiable'.

Sensitive information

3.143 'Sensitive information' is a sub-set of personal information and is given a higher level of protection under the NPPs. The IPPs do not refer to sensitive information and agencies are required to handle all information, including sensitive information, in accordance with the IPPs. This issue is discussed further in Chapter 19.

3.144 'Sensitive information' is defined in the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;

- membership of a trade union;
- sexual preferences or practices; or
- criminal record.

3.145 'Sensitive information' also includes health information[175] and genetic information about an individual that is not otherwise health information.[176]

3.146 'Sensitive information' is subject to a higher level of privacy protection than other 'personal information' handled by organisations in the following ways:

- 'sensitive information' may only be collected with consent except in specified circumstances. Consent is generally not required to collect 'personal information' that is not 'sensitive information';[177]
- 'sensitive information' must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;[178]
- 'sensitive information' cannot be used for the secondary purpose of direct marketing;[179] and
- 'sensitive information' cannot be shared by 'related bodies corporate' in the same way that they may share other 'personal information'.[180]

3.147 Similar classes of personal information are included in the definitions of 'sensitive information' in the Victorian, Tasmanian and Northern Territory privacy

175 *Privacy Act 1988* (Cth) s 6(1). The definition of 'health information' is discussed in Ch 57.

176 *Privacy Legislation Amendment Act 2006* (Cth). In the report *Essentially Yours* (ALRC 96), the ALRC and AHEC considered the definition of 'sensitive information'. They came to the conclusion that the definition did not provide an appropriate level of protection for genetic information that did not fall within the definition of health information—for example, genetic information derived from parentage or other identification testing that is not predictive of health—and recommended that the definition be amended to clarify this issue: Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–5. The Australian Government accepted this recommendation and the relevant amendment came into force in September 2006.

177 *Privacy Act 1988* (Cth) sch 3, NPP 10.

178 Ibid sch 3, NPP 2.1(a).

179 Ibid sch 3, NPP 2.1(c).

180 Ibid s 13B.

legislation.[181] Health information is not included in the definition of 'sensitive information' in Victoria because it is covered separately by the *Health Records Act 2001* (Vic). The *Privacy and Personal Information Protection Act 1998* (NSW) does not include a definition of sensitive information.

3.148 The Council of Europe Convention and OECD Guidelines do not specifically address sensitive information. Indeed, the Explanatory Memorandum to the OECD Guidelines expresses the view that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[182]

3.149 Article 8 of the EU Directive deals with 'special categories of data', which are defined as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. Article 8 prohibits the processing of this kind of information without consent except in specified circumstances and allows Member States to prohibit processing such data even with the consent of the data subject. The EU Directive also refers to 'sensitive data' but does not define the term.[183]

3.150 Sensitive information is provided with additional protection in the *Privacy Act* for a number of reasons. Information relating to race or ethnic origin, political or religious beliefs, trade union membership and sexual orientation, for example, is highly personal and may provide the basis for unjustified discrimination. In addition, this sort of information is likely to be necessary for the functions and activities of agencies and organisations in very limited circumstances. Health information, genetic information and criminal record information is also highly personal and has the potential to give rise to unjustified discrimination against individuals.

Submissions and consultations

Information made sensitive by context

3.151 In its submission to the Inquiry, the NHMRC stated that:

> it is extremely difficult to establish the categories of information which universally would be considered 'sensitive' either because of the nature of the information, the context in which it is handled or the views of the person to whom the information relates.
>
> We note that the *Personal Information Protection and Electronic Documents Act 2000* (Canada) does not define 'sensitive information' and that the Model Code allows an organisation discretion in determining whether information is sensitive. We

---

181 *Information Privacy Act 2000* (Vic) sch 1; *Personal Information Protection Act 2004* (Tas) s 3; *Information Act 2002* (NT) s 4. Note, however, that the Northern Territory Act does not specifically refer to 'an opinion' about those matters.

182 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19].

183 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 34, 70.

> also note that the sensitivity of certain categories of information may vary between cultures and individuals.[184]

3.152 The Canadian *Personal Information Protection and Electronic Documents Act 2000* states that:

> The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.[185]

3.153 The NHMRC suggested that:

> We support some regulatory discretion to prescribe categories of information, in addition to those that are included within the present definition contained in the *Privacy Act*, as sensitive information.[186]

3.154 The CSIRO suggested that sensitive information should include 'culturally sensitive data' or other data deemed to be sensitive by the data provider.[187]

3.155 The Queensland Government Commission for Children and Young People and Child Guardian noted that:

> For instance, a health practitioner receiving information relating to the abuse or neglect of a child may consider this information to be health information, and hence deal with it under the specific health privacy regime. However, if the same information is received by a child welfare practitioner it is not likely to be considered purely health information. The classification of child abuse information thus appears to depend not only on its nature, but also the context in which it is received.[188]

3.156 DLA Phillips Fox, however, supported the current definition of 'sensitive information':

> We also submit that the current definition of 'sensitive information' is adequate and appropriate. Introducing more subjective criteria (such as the sensitivity of the information taking into account surrounding circumstances) would:

---

184 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

185 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, cl 4.3.

186 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

187 CSIRO, *Submission PR 176,* 6 February 2007.

188 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

- result in greater uncertainty of application; and
- reduce the ability of organisations to implement broad guidelines for the treatment of categories of information so as to ensure compliance with the NPPs (and equivalent state and territory requirements).[189]

Financial information

3.157 The Australian Privacy Foundation suggested that sensitive information should include financial information.[190] A number of other stakeholders described consumer credit information as sensitive information.[191] The OPC stated that:

> Community attitudes research undertaken by the Office in 2001 and 2004 has indicated that individuals consider financial information to be very sensitive. In both community attitudes surveys, financial information was the top response for individuals when rating what types of information they were most reluctant to provide to organisations.[192]
>
> The Office believes that this issue warrants further exploration to determine whether financial information should be afforded the status of sensitive information. Where a decision is made to include financial information under the definition of sensitive information, financial information will need to be adequately defined under the Privacy Act. In general terms 'financial information' may mean account numbers or account details, pin numbers, income and asset information, bank statement information and so on. It would be important to clarify the limits of the definition of financial information in order to ensure that the definition of sensitive information would, in turn, be clear and straight-forward.[193]

3.158 Legal Aid Queensland, however, noted in its submission:

> That obtaining consent as the primary criteria for the release of financial information fails to recognise the inherent disparity in the bargaining positions of consumers and corporations.[194]

Biometric information

3.159 Biometric information can be 'personal information' for the purposes of the *Privacy Act* in some circumstances, that is, where an individual's identity is apparent or can reasonably be ascertained from the information. Biometric technologies are discussed further in Chapter 6. A number of stakeholders suggested that biometric information, like genetic information, should be accorded the higher protection

---

189 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.
190 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
191 J Harvey, *Submission PR 12,* 25 May 2006; National Legal Aid, *Submission PR 265,* 23 March 2007.
192 Office of the Privacy Commissioner, Community Attitudes Research 2001, 2004, available at <www.privacy.gov.au/business/research/index.html>.
193 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
194 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

provided by the *Privacy Act* in relation to 'sensitive information'.[195] Concern has been expressed that biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent,[196] and that biometric information could reveal other sensitive personal information, such as information about a person's health, racial or ethnic origin or religious beliefs.[197]

3.160 The Biometrics Institute describes the nature of biometric technology as follows:

> Biometric technology involves the storage and use of unique personal information to verify the identity of an individual. These unique identifiers are based on personal attributes such as fingerprints, DNA, iris, facial features, hand geometry, voice etc. Even a photograph could be described as one of the lower levels of biometric recognition.[198]

3.161 As discussed in Chapter 6, in a typical biometric system, a biometric device, such as a finger scanner, is used to take a biometric sample from an individual. Data from the sample are then analysed and converted into a biometric template, which is stored in a database or an object in the individual's possession, such as a smart card. Later biometric samples taken from the individual can then be compared to the stored biometric information to determine who the individual is (identification, or one-to-many matching) or to attempt to verify that an individual is who he or she claims to be (authentication, or one-to-one matching).

3.162 Recognising some of the special sensitivities around the use of biometric technology, the Biometrics Institute, in consultation with the OPC, has developed a privacy code to regulate the handling of biometric information.[199] The code binds private sector organisations that apply to become Code Subscribers and whose applications are approved by the Biometrics Institute Board. To date, only four organisations have elected to be bound by the Code. The Biometrics Institute has stated in relation to the Code:

> A Code can send a positive statement to the community that Biometrics Institute members are conscious of the privacy concerns of individuals and are prepared to voluntarily adopt higher standards for privacy protection than the National Privacy Principles (NPPs) require.

---

195 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007; AAMI, *Submission PR 147*, 29 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76*, 8 January 2007.

196 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12–13.

197 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 6; M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

198 Biometrics Institute, *Biometrics Institute Privacy Code Information Memorandum* (2006), 1.

199 Biometrics Institute, *Biometrics Institute Privacy Code* (2006).

> While the need for higher standards than those contained in the Privacy Act is debated by some Biometrics Institute members, there is a general consensus that a degree of public scepticism will need to be overcome before biometric systems are accepted as mainstream, or even privacy-enhancing.[200]

3.163 The *Biometrics Institute Privacy Code* includes a number of Supplementary Biometrics Institute Privacy Principles. One of the additional principles is similar in scope to the protection provided for 'sensitive information' by NPP 2.1(a):

> Secondary analysis or function creep of biometric information collected for purposes such as authentication or identification is not permitted without express free and informed consent. For example biometric information collected for the purposes of authentication and identification shall not be used to examine that information in search of genetic patterns or disease identification without express free and informed consent.[201]

3.164 In its submission to the Inquiry, the Health Informatics Society of Australia noted that:

> Sensitive information by definition relates to those areas where prejudices can prevail, eg sexual preferences, political or religious beliefs, criminal records, etc. The concern individuals have over the way that other parties might act based on the knowledge gained from genetic information puts this into the sensitive information category. Furthermore, biometric information can be considered sensitive since it is fixed and unlike a password or PIN cannot be reset once it has been inappropriately released.[202]

3.165 The OPC expressed the view that

> all biometric template information should be covered by the stricter provisions in the *Privacy Act* for sensitive information. However, it may be impractical and undesirable for all biometric samples to be included under the definition of sensitive information, especially where there is no intention to use the sample for biometric matching or identification. For example, it would be difficult and overly burdensome to require consent every time a photograph of a person (technically a biometric sample) is taken.
>
> The Office takes the view that sensitive information provisions should only apply to: (a) biometric samples collected for the purpose of biometric matching or biometric identification; and (b) biometric template information.
>
> The Office notes however that biometric samples—if they were to fall outside this definition of sensitive information—may still be covered by the *Privacy Act* as personal information and therefore achieve legislative protections. Furthermore, as noted in IP31 (at IP31 paragraph 11.46) there may be instances where a biometric sample reveals sensitive information about an individual such as health information and will thus be defined as sensitive information under the *Privacy Act*.[203]

---

200 Biometrics Institute, *Biometrics Institute Privacy Code Information Memorandum* (2006), 2–3.
201 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), 12.3.
202 Health Informatics Society of Australia, *Submission PR 196*, 16 January 2007.
203 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

ALRC's view

3.166 The ALRC recognises that personal information can become more or less sensitive because of the context in which it is considered and notes that this can apply to almost any personal information. The ALRC is not of the view, however, that the definition of 'sensitive information' should be amended to include information made sensitive by context. On balance, the existing approach of listing categories of information as sensitive provides greater certainty, which is important because the *Privacy Act* imposes more stringent requirements for handling sensitive information. In particular, the Act and the proposed UPPs provide that sensitive information should generally only be collected with consent and should be used only for the purpose for which the information was collected or a directly related secondary purpose. This regime is significantly different to the regime regulating the handling of other personal information, which can be collected without consent and used and disclosed for a broader range of purposes. It is important to be clear about what information is covered by the more stringent requirements.

3.167 It is also for this reason that the ALRC does not support the NHMRC's proposal to allow further categories of personal information to be added to those defined as sensitive by regulation. If the categories of information defined as sensitive are to be expanded, this should be done following full Parliamentary and community consideration and debate.

3.168 The ALRC's view is that financial information should not be included in the definition of sensitive information in the *Privacy Act*. Financial information is sensitive in some respects and does require appropriate handling, for example, appropriate security. Financial information has a number of characteristics, however, that set it apart from the categories of information currently included in the definition of sensitive information. It does not relate to the physical attributes or personal beliefs of the individual in the same way as other information currently defined as sensitive.

3.169 In addition, agencies and organisations often have a legitimate interest in an individual's financial information, for example, in relation to providing credit. Such information is necessary to the functions and activities of agencies and organisations in order to protect the interests of all parties to transactions. The *Privacy Act* already recognises that personal information relating to credit can be prejudicial and should only be collected, used and disclosed in appropriate circumstances. The Act provides a range of safeguards in relation to credit reporting that are discussed in detail in Part G. It is important to note, however, that these safeguards are not the same as the safeguards provided in relation to 'sensitive information'. For example, the credit reporting provisions do not require consent for the collection of credit information.

3.170 The ALRC is of the view, however, that the definition of sensitive information should be amended to include certain biometric information. Biometric information

shares many of the attributes of information currently defined as sensitive in the *Privacy Act*. It is very personal because it is information about an individual's physical self. Biometric information can reveal other sensitive information, such as health or genetic information and racial or ethnic origin. Biometric information can provide the basis for unjustified discrimination.

3.171 The ALRC recognises that requiring consent to collect all biometric information may be impracticable. For this reason, the ALRC has limited the type of biometric information to be included in the definition of sensitive information. The proposal below only includes biometric information collected for use in automated biometric authentication and identification systems and biometric template information. This proposal is intended to address the most serious privacy concerns around the handling of biometric information, for example, that such information may be used to identify individuals without their knowledge or consent.

3.172 The ALRC also proposes that the phrase 'sexual preferences and practices' currently used in the definition of 'sensitive information' should be changed to 'sexual orientation and practices'. The term 'sexual orientation' is consistent with language used in recent federal legislation[204] and state and territory anti-discrimination and human rights legislation[205] and reflects modern usage.

3.173 The ALRC notes that the provisions relating to sensitive information do not currently apply to agencies. In Chapter 19, the ALRC proposes that the UPPs dealing with 'sensitive information' apply to both agencies and organisations.[206] The ALRC also proposes in Chapter 19 to broaden the circumstances in which sensitive information may be collected without consent to include collection 'required or specifically authorised by or under law' to meet concerns raised by agencies.[207] Where biometric information is to be collected by agencies, for example, for inclusion in automated biometric authentication or identification systems, such as the 'SmartGate' automated border processing system,[208] such collection should be carried out on the basis of consent, or as required or specifically authorised by or under law.

---

204 *Private Health Insurance Act 2007* (Cth) s 55.5.

205 *Equal Opportunity Act 1995* (Vic) s 6; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 3; *Equal Opportunity Act 1984* (WA) s 35O; *Anti-Discrimination Act* 1998 (Tas) s 16; *Human Rights Act 2004* (ACT) s 8.

206 Proposal 19–1.

207 Proposal 19–2.

208 SmartGate is an automated border processing system. It performs the customs and immigration checks normally made by a Customs Officer on arrival in Australia. SmartGate takes a live image of an individual's face and using facial recognition technology matches that image with the digitised image stored in an ePassport.

Proposal 3–6 The definition of 'sensitive information' in the *Privacy Act* should be amended to include: (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information.

Proposal 3–7 The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.

Records

3.174 Generally, the privacy principles only apply to personal information that is held, or collected for inclusion, in a 'record'.[209] A record is defined as follows:

> (a) a document; or
>
> (b) a database (however kept); or
>
> (c) a photograph or other pictorial representation of a person;
>
> but does not include:
>
> (d) a generally available publication; or
>
> (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
>
> (f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or
>
> (fa) records (as defined in the *Archives Act 1983*) in the custody of the Archives (as defined in that Act) in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or
>
> (g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*; or
>
> (h) letters or other articles in the course of transmission by post.[210]

3.175 This section deals only with the first part of the definition, describing what is included in the definition of record. There were very few concerns raised about the second part of the definition, describing what is excluded from the definition of record,

---

209 Note, however, that the privacy principles also apply to information collected for inclusion in a 'generally available publication'. The definition of 'generally available publication' is discussed further below.

210 *Privacy Act 1988* (Cth) s 6(1).

apart from one issue raised by the OPC about the definition of 'generally available publication'. This issue is considered in the following section.

3.176 The first part of the definition includes electronic records about individuals such as social security records and doctors' records, and may also include photos or videos, where the person can be identified from the context or in other ways. A person's name appearing on a list of clients or patients may also fall within the definition of personal information because the context provides information, possibly sensitive personal information, about the individual.

3.177 The OPC commented that 'used in conjunction with definitions in the *Acts Interpretation Act 1901*, the definition for record is adequately broad to take in new or evolving information storage media'.[211] Section 25 of the *Acts Interpretation Act* provides:

> In any Act, unless the contrary intention appears:
>
> **document** includes:
>
> (a) any paper or other material on which there is writing;
>
> (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
>
> (c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.
>
> **record** includes information stored or recorded by means of a computer.
>
> **writing** includes any mode of representing or reproducing words, figures, drawings or symbols in a visible form.

3.178 The OPC made a number of suggestions for improving the definition of 'record', including amending the definition in order to clarify its scope and application to developing technology and allow it to 'stand alone'. The OPC also recommended the removal of the phrase 'of a person' from 'a photograph or other pictorial representation of a person' on the basis that a photograph may be 'personal information' even though it is not a photograph of a person. For example, a photograph of a house may be personal information if it is kept together with other information that identifies the resident.[212]

3.179 The *Privacy and Personal Information Act 1998* (NSW) covers information 'whether or not recorded in a material form'.[213] The Victorian and Tasmanian Acts include the requirement for information to be recorded in the definition of 'personal

---

211 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

212 The OPC also suggested that the definitions of 'record' and 'document' in the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) should be harmonised. This issue is discussed further in Ch 12.

213 *Privacy and Personal Information Protection Act 1998* (NSW) s 4.

information'. Personal information is defined as 'information or an opinion … that is recorded in any form'[214] and 'any information or opinion in any recorded format'.[215]

3.180 The Western Australian Information Privacy Bill provides an inclusive definition of 'record' that sets out essentially the same elements as the *Acts Interpretation Act* definition of 'document', plus the following additional elements:

- any map, plan, diagram or graph;
- any drawing, pictorial or graphic work, or photograph;
- any article on which information has been stored or recorded, either mechanically, magnetically or electronically.[216]

ALRC's view

3.181 The approach adopted in the Victorian and Tasmanian Acts—that is, including the requirement that information be recorded as part of the definition of 'personal information'—is not desirable. It excludes information that is being collected for inclusion in a record but has not yet been recorded, for example, information being collected orally from a health consumer by a health services provider.

3.182 The ALRC does not agree with the OPC that the definition of record needs to 'stand alone.' The long title of the *Acts Interpretation Act* is 'An Act for the Interpretation of Acts of Parliament and for Shortening their Language.' It is appropriate to rely on the definitions provided in that Act unless the Australian Parliament intends a particular term to have a meaning that is different from the meaning set out in the *Acts Interpretation Act.* This promotes consistency and brevity in federal legislation.

3.183 The term 'record' is defined in the *Acts Interpretation Act*. It includes 'information stored or recorded by means of a computer'. The ALRC's view is that this definition is not sufficient in the context of the *Privacy Act.* It does not give an indication of the intended broad scope of the *Privacy Act*, which is not limited to information stored on computer. It is therefore appropriate to define the term separately and to include a reference to information stored in electronic or other forms. The ALRC's view is that the definition of record in the *Privacy Act* should be inclusive rather than exhaustive.

---

214 *Information Privacy Act 2000* (Vic) s 3.
215 *Personal Information Protection Act 2004* (Tas) s 3.
216 Information Privacy Bill 2007 (WA) cl 4.

3.184 The term 'document' is also defined in the *Acts Interpretation Act.* This definition is appropriate and should be incorporated in the definition of record in the *Privacy Act* by reference.

3.185 The ALRC agrees with the OPC that photographs or other pictorial representations should be covered by the term 'record' in the *Privacy Act* and that they should not be limited by the phrase 'of a person'. This can be achieved by relying on the definition of 'document' in the *Acts Interpretation Act*, which includes 'any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device'. The term 'images' is wide enough to cover photographs and other pictorial representations. If this approach is adopted, existing paragraph (c) of the definition of record in the *Privacy Act* is not needed.

Proposal 3–8 The definition of 'record' in the *Privacy Act* should be amended in part to include: (a) a document; and (b) information stored in electronic or other forms.

Generally available publications

3.186 The definition of 'record' in the *Privacy Act* excludes a range of things such as items kept in libraries, art galleries or museums for reference, study or exhibition; a range of Commonwealth archival records, including those in the open access period; documents in the memorial collection of the Australian War Memorial and letters and other articles in the course of transmission by post. There were very few concerns raised with these elements of the definition and the ALRC does not propose any changes to them.

3.187 The definition of 'record' in the *Privacy Act* also excludes 'generally available publications'—that is, 'a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public'. It is important to note, however, that the collection of personal information for inclusion in a generally available publication is regulated by the privacy principles.[217]

3.188 The OPC commented in its submission that:

> The Office notes that the phrase 'generally available publication' may appear to apply only to publications that do not involve fees for access. However, access to generally available publications is not necessarily free. For example, the National Insolvency Index is accessible only by subscribers who pay to view the Index.

217 *Privacy Act 1988* (Cth) ss 14, 16B.

> For this reason, the Office believes that the definition would benefit from the clarification that a generally available publication is generally available even where payment of a fee is necessary to access the information.[218]

ALRC's view

3.189 The ALRC notes that a great number of generally available publications are only available for a fee including those examples expressly included in the current definition such as books and magazines. The ALRC sees merit in clarifying that a publication is 'generally available' whether or not a fee is charged for access to the publication.

Proposal 3–9 The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

Deceased individuals

3.190 With the exception of Part VIA dealing with declared disasters and emergencies, the *Privacy Act* does not protect the personal information of deceased individuals. The term 'individual' is defined as 'a natural person'.[219] The OPC review stated that:

> The term 'natural person' is not defined under the *Privacy Act* or the *Acts Interpretation Act 1901*; however it appears the term is usually used to distinguish human beings from artificial persons or corporations. Whether the term 'natural persons' includes a deceased human being does not appear to have been subject to judicial consideration in Australia or the United Kingdom. The Office considers the term 'natural person' to mean a living human being as this is the plain English meaning of the term.[220]

3.191 Paul Roth notes that:

> It is normally accepted that in law, deceased persons have no privacy interests. This is presumably on the basis that the *raison d'être* for privacy protection no longer exists, since dead people can feel no shame or humiliation. The underlying common law principle here is much the same as in the law of defamation, which in most jurisdictions does not countenance civil actions that seek to vindicate the reputation of the dead.[221]

---

218 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

219 *Privacy Act 1988* (Cth) s 6(1).

220 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 281.

221 P Roth, 'Privacy Proceedings and the Dead' (2004) 11 *Privacy Law & Policy Reporter* 50.

3.192 Part VIA of the *Privacy Act*—dealing with personal information in declared emergencies and disasters—explicitly states, however, that for the purposes of Part VIA, the definition of 'personal information' 'is taken to include a reference to an individual who is not living'. The provisions in Part VIA displace some of the requirements in the IPPs and NPPs by providing a separate regime for the collection, use and disclosure of personal information in the case of a declared emergency. The aim of Part VIA is to enhance information exchange between Australian Government agencies, state and territory authorities, organisations, non-government organisations and others, in emergencies and disasters. The provisions are discussed in detail in Chapter 40.

3.193 The OPC makes the following suggestion in relation to the 'personal information' of deceased individuals:

> Although information about dead people is not technically considered to be personal information, Agencies are encouraged to respect the sensitivities of family members when using or disclosing it.[222]

Freedom of Information and Archives Acts

3.194 The *Freedom of Information Act 1982* (Cth) (the FOI Act) establishes a legally enforceable right of access to documents held by Australian Government public sector agencies. The Act sets out a number of exceptions to that right of access and these are described as 'exempt documents'. One class of exempt document is as follows:

> A document is an exempt document if its disclosure under this Act would involve the unreasonable disclosure of personal information about any person (including a deceased person).[223]

3.195 Where a request is made for access to the personal information of a deceased individual held by an agency and it appears to the decision maker under the FOI Act that the legal personal representative of the person might reasonably wish to contend that the document should not be released, the representative must be given a reasonable opportunity to make submissions in relation to the matter.[224] Where a decision is made that the personal information of a deceased individual is to be released under the FOI Act, the legal personal representative of the deceased person may apply to the Administrative Appeals Tribunal for review of the decision.[225] The FOI Act does not provide for amendment or annotation of personal information by a third party on behalf of a deceased individual.

---

222 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 3.

223 *Freedom of Information Act 1982* (Cth) s 41(1). There are similar provisions in state and territory legislation. See, eg, *Freedom of Information Act 1989* (NSW) sch 1, pt 2 cl 6(1); *Freedom of Information Act 1982* (Vic) s 33(1); *Freedom of Information Act 1989* (ACT) s 41(1).

224 *Freedom of Information Act 1982* (Cth) s 27A. Legal personal representative includes the executor or administrator of a deceased individual's estate.

225 Ibid s 59A.

3.196 Once records are no longer required to be readily available to an agency, most agencies are required to transfer the records to the National Archives of Australia. The *Archives Act* deals with storage, disposal and destruction of such records. The Act also provides that, once records are 30 years old and in the open access period, they should be made available to the public except in some circumstances. These include where they contain

> information or matter the disclosure of which under this Act would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person).[226]

3.197 Thus, while both the FOI Act and the *Archives Act* provide avenues for third parties to apply for access to information about deceased individuals, agencies are required to consider whether releasing the information would amount to an 'unreasonable' disclosure.

State and territory legislation

3.198 Some New South Wales and Victorian privacy legislation covers personal information about individuals who have been dead for not more than 30 years.[227] This reflects the 30 year period after which government archival records are generally open to public access.[228] The Northern Territory *Information Act*, which combines privacy, freedom of information and archives provisions, covers personal information within the first five years after an individual dies.[229] Tasmanian privacy legislation extends to the personal information of individuals who have been dead for not more than 25 years,[230] and ACT health privacy legislation covers deceased individuals without imposing any time restrictions.[231]

3.199 A number of these Acts contain arrangements to address the situation where a decision is required by an individual in relation to his or her personal information under the Act, but the individual does not have capacity to make the decision. These arrangements extend to individuals who are unable to make decisions because they have died. Under the New South Wales *Health Records and Information Privacy Act*, for example, an 'authorised representative' may make decisions on behalf of a deceased individual.[232] 'Authorised representative' includes 'a person who is otherwise

---

226 *Archives Act 1983* (Cth) s 33(1)(g).
227 *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a); *Health Records and Information Privacy Act 2002* (NSW) s 5(3)(a); *Health Records Act 2001* (Vic) ss 3(1), 95.
228 *Archives Act 1983* (Cth) s 3(7).
229 *Information Act 2002* (NT) s 4.
230 *Personal Information Protection Act 2004* (Tas) s 3.
231 *Health Records (Privacy and Access) Act 1997* (ACT) ss 4, 27 and dictionary (definition of 'consumer').
232 *Health Records and Information Privacy Act 2002* (NSW) s 7.

empowered under law to exercise any functions as an agent of or in the best interests of the individual',[233] including an executor or administrator of a deceased estate.

Duty of confidentiality

3.200 A legal duty of confidentiality may arise in equity, at common law or under contract and provides some protection for personal information provided in confidence. How such duties arise and their consequences are discussed in Chapter 12. A duty of confidence ends when the information loses its quality of confidence, whether through the passage of time, loss of secrecy or other change of circumstances.[234] This does not mean, however, that the duty necessarily ends when the person who has provided the information dies. The law of confidentiality, therefore, may provide some protection for the personal information of deceased individuals where that personal information was provided in confidence to banks, lawyers, doctors and others.

Genetic information

3.201 In the report *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96), the ALRC and the Australian Human Ethics Committee (AHEC) of the NHMRC recommended that:

> The Commonwealth should amend the *Privacy Act* to provide that 'health information' includes information about an individual who has been dead for 30 years or less. These amendments should include provision for decision making by next-of-kin or an authorised person in relation to the handling of a deceased individual's health information.[235]

3.202 The policy justification for extending the protection of the *Privacy Act* to the genetic information of deceased individuals is that this information may have implications for living genetic relatives.[236] The Australian Government noted in its response to ALRC 96 that this recommendation was being considered in the context of the development of the *National Health Privacy Code*.[237] The draft *National Health Privacy Code* is expressed to apply to the health information of individuals who have been dead for not more than 30 years.[238]

The OPC review

3.203 The OPC review noted that extending the Act to cover the personal information of deceased individuals would require some reworking of provisions and principles

---

233 Ibid s 8.

234 R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006), 117.

235 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–6.

236 Ibid, [7.90].

237 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 30 July 2007.

238 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4. The Code is discussed further in Ch 56.

relating to consent and the lodging of complaints. The OPC review recommended that this issue be considered in the context of a wider review of the Act.[239]

Submissions and consultations

3.204 A number of submissions highlighted problems in this area. One stakeholder was distressed at being contacted by direct marketing companies attempting to contact her deceased husband.[240] Another stakeholder expressed concern about an insurance company seeking to collect health information about an individual from the individual's next of kin in the mistaken belief that the individual was deceased.[241]

3.205 There was significant support expressed in submissions and consultations for extending at least some privacy principles to the personal information of deceased individuals.[242] A number of stakeholders expressed the view that the principles should only apply so far as practicable.[243]

3.206 In its submission to this Inquiry, the Australian Privacy Foundation noted that there are good arguments both for and against extending privacy rights to cover the personal information of deceased individuals. The Foundation noted that not all the privacy principles sensibly apply to the personal information of deceased individuals—since the person cannot be notified or consulted about how his or her personal information is handled—and that it might be preferable to write specific provisions to address this issue, rather than simply extend the definition of 'personal information' to include the personal information of deceased individuals.[244]

3.207 The Commonwealth Ombudsman noted that it

> has had to deal with occasional issues relating to deceased people—one example being medical records of Defence personnel. Different standards apply under FOI (where exempt personal information can relate to a deceased person) and privacy (where the legislation does not require it but where OFPC suggests a cautious

239 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 85.

240 A Baxter, *Submission PR 74*, 5 January 2007.

241 Confidential, *Submission PR 223*, 8 March 2007.

242 Australian Government Department of Health and Ageing, *Submission PR 273*, 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171*, 5 February 2007; Australian Institute of Health and Welfare, *Submission PR 170*, 5 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007; Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

243 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AAMI, *Submission PR 147*, 29 January 2007.

244 Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

> approach). A commonsense approach might be to permit disclosure of sensitive information only where there is a balance of public interest in doing so.[245]

3.208 The Centre for Law and Genetics expressed support for extending the *Privacy Act* to cover the personal information of deceased individuals and noted that the justification is particularly strong in relation to Indigenous communities because those communities have 'religious and spiritual concerns about representations of deceased individuals'.[246]

3.209 AAMI expressed support for extending the *Privacy Act* to cover the information of deceased individuals:

> AAMI often sadly is dealing with a deceased person's information, mainly as a result of a fatality claim on a motor vehicle insurance policy or as part of a compulsory third party (CTP) claim. AAMI currently applies its privacy protection procedures to the deceased personal information as it would to a natural person, as far as is practicable. Therefore AAMI supports amending the Act to include personal information of the deceased, with the provision that in certain circumstances it may not be practicable.[247]

3.210 Other organisations also noted that, for simplicity or in order to comply with state and territory legislation, they handled the personal information of deceased individuals in the same way as they handled the personal information of living individuals.[248] The Australian Government Department of Community Services expressed support for covering the personal information of deceased individuals and noted that the secrecy provisions included in Medicare and Centrelink legislation continued to cover individuals after death.[249] Part 5 of the Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007, which deals with the confidentiality of information collected in relation to the proposed access card, defines 'protected information' as 'information relating to an individual (living or dead)'.[250]

3.211 The NHMRC stated that:

> The present situation, whereby the health information of deceased persons is protected by legislation in several States and Territories but not by Commonwealth legislation adds to the complexity and confusion created by the existing regulatory regime; and
>
> Information about the health of deceased persons, in particular but not limited to genetic information, may have significant implications for living relatives, both genetic and non-genetic. It is preferable for representatives of the deceased to be able to consent to collection, use and disclosure of such information.[251]

---

245 Commonwealth Ombudsman, *Submission PR 202*, 21 February 2007.

246 Centre for Law and Genetics, *Submission PR 127*, 16 January 2007. See also the discussion of the particular privacy needs of Indigenous people in Ch 1.

247 AAMI, *Submission PR 147*, 29 January 2007.

248 National Australia Bank and MLC Ltd, *Submission PR 148*, 29 January 2007; AXA, *Submission PR 119*, 15 January 2007.

249 Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007.

250 Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 89.

251 National Health and Medical Research Council, *Submission PR 114*, 15 January 2007.

3.212 Some concerns were raised about extending the *Privacy Act* to include the personal information of deceased individuals. These included: increased complexity for executors, family members and insurance companies following the death of an individual;[252] more limited access to information for research and other activities of interest to family members or in the public interest;[253] and an additional compliance burden for business.[254]

3.213 The Australian Federal Police did not support extending the *Privacy Act* to cover the personal information of deceased individuals because of the potential to complicate their investigations relating to deceased individuals.[255] The Australian Tax Office stated that:

> In our view, there may be some justification for expanding the definition to include information about the deceased, particularly health and medical information. However, we would be hesitant to recommend any changes that would restrict the way that regulatory and enforcement agencies can access information about the deceased to maintain up-to-date and accurate registers. The ability to collect and use information about deceased persons helps us to keep our taxpayer records as accurate as possible. Access to this information is also a key way of combating identity fraud as it helps to prevent 'new' identities being registered using details of the deceased.[256]

3.214 A number of stakeholders also commented on the difficulties that arise when it is necessary to seek decisions on behalf of deceased individuals from alternative decision makers. One submission noted that family members do not speak with one voice on such matters.[257] Other stakeholders noted that obtaining consent can be difficult especially where there is a dispute in the family[258] and that it becomes more difficult to identify and locate alternative decision makers as time passes.[259] Where it is not possible to identify and locate an alternative decision maker, this may mean that information cannot be collected, used or disclosed.

3.215 The State Records Office of Western Australia commented that concerns about sensitive personal information of deceased individuals tend to diminish over time.[260] The Privacy Committee of South Australia noted that, in dealing with the personal

---

252 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.
253 Government of South Australia, *Submission PR 187,* 12 February 2007; Australian Institute of Health and Welfare, *Submission PR 170,* 5 February 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.
254 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
255 Australian Federal Police, *Submission PR 186,* 9 February 2007.
256 Australian Taxation Office, *Submission PR 168,* 15 February 2007.
257 Public Record Office Victoria, *Submission PR 72,* 3 January 2007.
258 Banking and Financial Services Ombudsman, *Consultation PC 76,* Melbourne, 5 February 2007.
259 B Armstrong, *Consultation PC 47,* Sydney, 10 January 2007.
260 State Records Office of Western Australia, *Consultation PC 67,* Perth, 24 January 2007.

information of deceased individuals, it was necessary to balance privacy concerns with what is reasonable and what is in the public interest.[261]

ALRC's view

3.216 Currently, when someone dies, his or her personal information is no longer subject to the provisions of the *Privacy Act*, apart from Part VIA dealing with declared emergencies and disasters. Access to the personal information of a deceased individual in the Australian Government public sector is governed by the FOI Act and the *Archives Act*. Access to personal information in the private sector may be subject to state or territory legislative requirements, a duty of confidentiality or simply dealt with as a matter of organisational policy.

3.217 While there was significant support among stakeholders for extending the *Privacy Act* to cover the personal information of deceased individuals, submissions and consultations did not indicate that there were widespread problems caused by the current lack of coverage. Some specific problems were identified, including the use of inaccurate and out-of-date personal information and the need to allow access to genetic information for genetic relatives.

3.218 In the ALRC's view, the personal information of deceased individuals should be expressly addressed in the *Privacy Act* and that some provision should be made for the use and disclosure of that information in appropriate circumstances.

3.219 The ALRC does not believe, however, that it is appropriate simply to extend the definition of 'personal information' in the Act to include the personal information of deceased individuals. It is clear that not all the privacy principles can be applied sensibly, or applied in full, to the personal information of deceased individuals. Instead, the *Privacy Act* should be amended to make specific provision for dealing with the personal information of deceased individuals.

3.220 In the ALRC's view, the *Privacy Act* should be amended to include a new Part setting out a number of provisions dealing specifically with the handling of the personal information of deceased individuals. The new Part should apply only to organisations and to information about individuals who have been dead for 30 years or less.

3.221 In relation to agencies, access to personal information of deceased individuals should continue to be regulated by the FOI Act and the *Archives Act.* The archiving and destruction of personal information of deceased individuals held by agencies should continue to be regulated by the *Archives Act.*

261 Privacy Committee of South Australia, *Consultation PC 110*, Adelaide, 1 March 2007.

Decisions on behalf of deceased individuals

3.222 As discussed above, some state and territory privacy legislation makes provision for decisions to be made by third parties on behalf of deceased individuals. This issue also arises under the *Privacy Act*. For example, NPP 2 requires consent to use personal information for a secondary purpose that is unrelated to the primary purpose of collection and outside the reasonable expectations of the individual. The ALRC is not proposing, however, that the *Privacy Act* be amended to provide for decisions to be made by third parties on behalf of deceased individuals.

3.223 The ALRC notes that where there is a request to access the personal information of a deceased individual under the FOI Act, the Act requires agencies to provide a deceased individual's legal personal representative with a reasonable opportunity to make submissions in relation to that request. The agency, however, retains the power to make the decision on whether access is granted.

3.224 In considering whether to impose an obligation on organisations to consult with third parties, or a requirement to seek a decision from a third party on behalf of a deceased individual, the ALRC considered the difficulties with these processes highlighted by stakeholders and the likely compliance costs such processes would impose on organisations. On balance, the ALRC considers that such an obligation or requirement should not imposed on organisations.

3.225 Instead, the ALRC proposes that organisations should be required to consider whether a proposed use or disclosure of the personal information of a deceased individual would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. In making this decision, organisations may find it useful to consult the individual's family or legal personal representative, but the ALRC does not propose that there be a legal requirement to do so.

3.226 In relation to health information, in particular, the ALRC's view is that one individual or family member should not be able to stop another family member from gaining access to a deceased family member's information. Family members often have different views on the appropriateness of access to information or the sensitivity of that information. In ALRC 96, the ALRC and AHEC noted that:

> If the law requires that access to genetic information about a deceased individual can be granted only with the consent of that person's legal or other authorised representative, genetic relatives may still have problems in gaining access.[262]

262 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.93].

Use and disclosure

3.227 The *Privacy Act* should specify that organisations must only use or disclose the personal information of deceased individuals in accordance with the proposed 'Use and Disclosure' principle. Where such use or disclosure would require consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. This is consistent with the test imposed on agencies under the FOI Act relating to the release of information in response to an access request. The test of what amounts to 'unreasonable disclosure' has been considered in the FOI context:

> The application of the test involves a consideration of all the factors relevant in a particular case and a balancing of all legitimate interests (*Wiseman v. Commonwealth*, (D251) eg *Re Chandra and Minister for Immigration and Ethnic Affairs* (D33)).[263]

3.228 The ALRC's view is that there are circumstances in which it would be reasonable for organisations to use or disclose the personal information of deceased individuals for a secondary purpose unrelated to the primary purpose of collection, for example, in the administration of a deceased estate or in response to a request from a family member undertaking family history research. In considering all the factors relevant to a particular case and balancing all legitimate interests, organisations will need to consider issues such as any existing duty of confidentiality to the deceased individual, the interests of family members and any public interest in the use or disclosure. In some circumstances it may be important to contact family members or the deceased individual's legal personal representative in order to be able to make an informed decision about what is reasonable.

3.229 This same test should also be applied to the use or disclosure of sensitive information.[264] Where consent to use or disclose sensitive information would be required—that is, where the secondary purpose is not directly related to the primary purpose of collection or the individual would not reasonably expect the organisation to use or disclose the information for that secondary purpose—organisations should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of sensitive information about any person, including the deceased person. In considering what is reasonable, the organisation would be required to consider the sensitivity of the information.

Access

3.230 Organisations should be required to consider providing third parties with access to the personal information of deceased individuals in accordance with the access

---

263 Australian Government Attorney-General's Department, *Freedom of Information Memorandum 98: Exemption Sections in the FOI Act* (2005).

264 Health information of deceased individuals is discussed further below.

elements of the proposed 'Access and Correction' principle. Organisations should be required to consider in each case whether providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

Correction

3.231 In the ALRC's view, a third party should not have a right to seek to correct the personal information of a deceased individual under the *Privacy Act*. This is consistent with the position under the FOI Act. In relation to the personal information of deceased individuals, the proposed 'Data Quality' principle, discussed below, would operate to ensure that information is kept accurate, complete, up-to-date and relevant. In order to comply with the Data Quality principle, an organisation would be required to consider information provided by third parties relating to the personal information of a deceased individual.

Data Quality

3.232 Organisations should be required to ensure that the personal information of deceased individuals is accurate, complete, up-to-date and relevant to any proposed use or disclosure, before they use or disclose the information. This should help to ensure that surviving family members do not continue to receive correspondence addressed to the deceased individual.

Data security

3.233 Organisations should be required to take reasonable steps to protect the personal information of deceased individuals from misuse and loss and from unauthorised access, modification or disclosure. Organisations should be required to take reasonable steps to destroy or render personal information of deceased individuals non-identifiable, if it is no longer needed for a purpose permitted under the proposed UPPs.

3.234 Organisations should be required to take reasonable steps to ensure that personal information of deceased individuals it discloses to a person pursuant to contract, or otherwise in connection with the provision of a service, is protected from being used or disclosed by that person otherwise than in accordance with the proposed UPPs.

Health information

3.235 In ALRC 96, the ALRC and AHEC recommended that the definition of 'health information' in the *Privacy Act* be amended to include information about an individual

who has been dead for 30 years or less and that these amendments should include provision for decision making by next-of-kin or an authorised person.[265]

3.236 The ALRC is of the view that the provisions discussed above should also apply to the health information, including the genetic information, of deceased individuals. For the reasons discussed above, however, the ALRC no longer supports requiring decisions to be made by third parties on behalf of deceased individuals.

3.237 In Chapter 57 the ALRC considers NPP 2.1(ea) in relation to the use or disclosure of an individual's genetic information to a genetic relative. NPP 2.1(ea) allows an organisation to use or disclose an individual's genetic information where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the individual. NPP 2.1(ea) also provides that any such use or disclosure must be in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner. In Chapter 57, the ALRC proposes that this provision be amended to replace the reference to guidelines issued by the NHMRC with a reference to rules issued by the Privacy Commissioner. It is also proposed that the provision be moved to the proposed *Privacy (Health Information) Regulations*.

3.238 It is anticipated that the proposed rules will address issues such as providing access to genetic information by making the information available to the genetic relative's nominated medical practitioner or genetic counsellor, who can explain the clinical relevance of the information. Any use or disclosure of genetic information of a deceased individual should also be conducted in accordance with these rules.

3.239 On the basis of the proposed provisions relating to deceased individuals, discussed above, a genetic relative would be able to apply for access to the genetic information of a deceased individual. An organisation would then be required to consider whether the proposed use or disclosure of the information would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

3.240 It should be made clear, in the proposed provisions dealing with the personal information of deceased individuals, that it is reasonable for an organisation to use or disclose genetic information to a genetic relative where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative. In addition, the provision should provide that, where an organisation decides to disclose the genetic information of a deceased individual to a genetic relative, that disclosure must be in accordance with the rules issued by the Privacy Commissioner.

---

265 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–6.

Complaints

3.241 The ALRC's view is that a breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act* and that it should be possible to lodge a complaint with the Privacy Commissioner in relation to any such alleged interference with privacy. The complaint process should parallel, as far as possible, the process provided for complaints by living individuals about their personal information.

3.242 The following individuals should have standing to lodge a complaint about the handling of the personal information of a deceased individual. In relation to an alleged breach of the use and disclosure, data quality or data security provisions, the ALRC is of the view that the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner[266] or legal personal representative should have standing to allege an interference with privacy. In relation to a request for access to the personal information of a deceased individual, the ALRC's view is that any person who has made a request for access to the personal information of a deceased individual should have standing to allege an interference with privacy.

3.243 These proposed changes will provide a regime in which organisations can disclose the personal information of deceased individuals in appropriate circumstances and third parties can get access to the personal information of deceased individuals where it is reasonable for them to do so.

Proposal 3–10 The personal information of deceased individuals held by agencies should continue to be regulated by the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth).

Proposal 3–11 The *Privacy Act* should be amended to include a new Part dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The new Part should provide as follows:

266 The ALRC proposes that the term 'de facto spouse' in the *Privacy Act* be changed to 'de facto partner': at Proposal 57–4.

(a) Use and disclosure

Organisations should be required to use or disclose the personal information of deceased individuals in accordance with the proposed 'Use and Disclosure' principle in the UPPs. Where the principle requires consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to consider providing third parties with access to the personal information of deceased individuals in accordance with the access elements of the proposed 'Access and Correction' principle in the UPPs. Organisations should be required to consider in each case whether providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data quality

Organisations should be required to ensure that the personal information of deceased individuals is, with reference to a use or disclosure permitted under the UPPs, accurate, complete, up-to-date and relevant before they use or disclose the information.

(d) Data security

Organisations should be required to take reasonable steps to protect the personal information of deceased individuals from misuse and loss and from unauthorised access, modification or disclosure.

Organisations should be required to take reasonable steps to destroy or render personal information of deceased individuals non-identifiable if it is no longer needed for any purpose permitted under the proposed UPPs.

Organisations should be required to take reasonable steps to ensure that personal information of deceased individuals they disclose to a person pursuant to contract, or otherwise in connection with the provision of a service, is protected from being used or disclosed by that person otherwise than in accordance with the *Privacy Act*.

Proposal 3–12 The proposed provisions dealing with the use or disclosure of personal information of deceased individuals should make clear that it is reasonable for an organisation to use or disclose genetic information to a genetic relative of a deceased individual where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. Any use or disclosure of genetic information of deceased individuals should be in accordance with rules issued by the Privacy Commissioner.

Proposal 3–13 Breach of the proposed provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner alleging an interference with the privacy of a deceased individual:

(a) in relation to an alleged breach of the use and disclosure, data quality or data security provisions, the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner or legal personal representative; and

(b) in relation to an alleged breach of the access provision, any person who has made a request for access to the personal information of a deceased individual.

4. Achieving National Consistency

Contents

Introduction 235
The federal system 237
Is national consistency important? 238
National legislation 241
Constitutional issues 242
Submissions and consultations 245
Commonwealth-state cooperative scheme 247
Submissions and consultations 251
A model for national consistency 253
National legislation 253
A Commonwealth-state cooperative scheme 258
Other options 260
A review 261
A permanent standing body 262
Options for reform 263
Submissions 264
ALRC's view 265
A single privacy regulator? 267
Submissions 268
ALRC's view 269
Other methods to achieve national consistency 270
Binding codes 271
Non-binding guidelines 272
Rules, codes and guidelines 272
Guidance on the interaction of legislation 273
Scrutiny of legislation 274
Privacy impact statements and assessments 274

Introduction

4.1 In its 1983 report *Privacy* (ALRC 22), the ALRC proposed a national approach to the protection of privacy 'at the very least in relation to information practices'.[1] Australia is yet to achieve uniformity in the regulation of personal information. A key

1 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1092].

issue raised in recent inquiries[2] and the current ALRC Inquiry,[3] is that Australian privacy laws are multi-layered, fragmented and inconsistent. For example, the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth) (Senate Committee privacy inquiry) concluded that:

> The committee is greatly concerned at the significant level of fragmentation and inconsistency in privacy regulation. This inconsistency occurs across Commonwealth legislation, between Commonwealth and state and territory legislation, and between the public and private sectors. As mentioned above, the committee believes that this inconsistency is one of a number of factors undermining the objectives of the Privacy Act and adversely impacting on government, business, and mostly importantly, the protection of Australians' privacy.[4]

4.2 The various problems caused by inconsistency and fragmentation in privacy regulation are outlined in Part C of this Discussion Paper. This chapter outlines a number of proposals for reform to deal with inconsistency and fragmentation in the regulation of privacy. The chapter first considers whether national consistency should be one of the goals of the regulation of personal information. It then considers various mechanisms for achieving consistency at the federal, state and territory level. These include: the Australian Parliament legislating to the exclusion of the states and territories in relation to the handling of personal information in the private sector; privacy legislation that is consistent with the *Privacy Act* regulating state and territory public sectors; and the establishment of a permanent standing body to monitor and ensure continuing national consistency. The final section of the chapter considers

---

2 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.17]–[4.40] and recs 3, 4; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Ch 2 and recs 2–16; Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), Ch 4 and recs 4.47, 4.48.

3 Inconsistency in the regulation of personal information has been raised as an issue in a large number of submissions to, and consultation meetings with, the ALRC. See, eg, Health and Community Services Complaints Commission (South Australia), *Submission PR 207,* 23 February 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; G Hill, *Consultation PC 21*, Melbourne, 8 May 2006; NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006; B Bainbridge, *Consultation PC 12*, Canberra, 30 March 2006; Commonwealth Ombudsman, *Consultation PC 11*, Canberra, 30 March 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006; D Giles, *Consultation PC 6*, Sydney, 2 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

4 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.6].

various other methods for achieving national consistency including binding codes, guidelines, privacy impact assessments and scrutiny of legislation.

The federal system

4.3 The *Australian Constitution* establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. Section 109 of the *Australian Constitution* provides that: 'when a law of a State is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid'. This provision may operate in two ways: it may directly invalidate state law where it is impossible to obey both the state law and the federal law;[5] or it may indirectly invalidate state law where the Australian Parliament's legislative intent is to 'cover the field' in relation to a particular matter.[6]

4.4 It has been observed that inconsistency in the regulation of personal information stems largely from the failure of federal law to 'cover the field'.[7] Section 3 of the *Privacy Act* states:

> It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

4.5 The provision makes clear that the Australian Parliament did not intend to 'cover the field' or to override state and territory laws relating to the protection of personal information, if such laws are capable of operating alongside the *Privacy Act*. Section 3 of the *Privacy Act* does not, however, sit comfortably with s 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth), which states that one of the objects of the Act is

> to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations.[8]

4.6 A number of the states and territories have enacted privacy regimes. In particular, different privacy regimes regulate the handling of personal information in state and territory public sectors. In some states and territories personal information is regulated by legislative schemes, in others by administrative regimes. These regimes

---

5 *Australian Boot Trade Employees Federation v Whybrow & Co* (1910) 10 CLR 266; *R v Licensing Court of Brisbane; Ex parte Daniell* (1920) 28 CLR 23.

6 *Clyde Engineering Co Ltd v Cowburn* (1926) 37 CLR 466.

7 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.21].

8 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3(a).

are sometimes inconsistent with the *Privacy Act* and with each other.[9] Further, New South Wales (NSW), Victoria and the ACT all have legislation that regulates the handling of personal health information in the private sector. This means that health service providers and others in the private sector in those jurisdictions are required to comply with both federal and state or territory legislation.[10]

4.7 Chapters 2 and 14 note that although the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs) and privacy principles under state and territory privacy regimes are similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs. As noted in Chapter 15, there are significant differences between the IPPs and the NPPs.

4.8 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96) the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council considered whether the NSW, Victorian and ACT health privacy legislation might be inconsistent with the *Privacy Act* and to that extent invalid.[11] The Australian Government Attorney-General's Department stated in its submission to that inquiry that s 3 of the *Privacy Act* was not intended to enable state and territory law to regulate the same types of personal information and organisations that are regulated by the *Privacy Act*. Privacy NSW, on the other hand, submitted that the states should be free to 'enhance the Commonwealth's minimum standards in state legislation'.[12]

4.9 The Office of the Privacy Commissioner (OPC) review of the private sector provisions of the *Privacy Act* (OPC Review) recommended that:

> The Australian Government should consider amending section 3 of the *Privacy Act* to remove any ambiguity as to the regulatory intent of the private sector provisions.[13]

Is national consistency important?

4.10 A threshold issue is whether national consistency in the regulation of personal information is important.[14] In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether national consistency was desirable or whether there were circumstances that justified some level of inconsistency.

---

9 See discussion in Ch 2.

10 For further discussion of national consistency in the regulation of health information, see Part H.

11 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

12 Ibid, [7.44]–[7.49].

13 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 2.

14 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 2–1.

4.11 All submissions that addressed this issue strongly supported national consistency.[15] Most focused on how a nationally consistent privacy regime would lessen unjustified compliance burden and cost. For example, a number of stakeholders emphasised that national consistency is essential to lessen the compliance burden for organisations and agencies that operate across state borders.[16] A large number of submissions identified that state and territory legislation regulating the handling of personal information in the private sector is a major cause of inconsistency, complexity and costs.[17] Other submissions noted that the use of technologies—such as the internet—justifies a harmonised approach to privacy regulation at both a national and international level.[18] These issues are discussed in more detail below and in Chapter 11.

4.12 Some stakeholders noted, however, that while national consistency is a valuable objective, it should not be pursued to the detriment of the level of protection afforded by privacy legislation.[19] The OPC submitted that:

> Consistency does not mean the elimination of multi-layered regulation. In many cases, additional protections that regulate particular sectors, or protect certain information, can enhance privacy (such as privacy codes and secrecy provisions). However, in the interests of all parties, it is critical to ensure these layers are not unnecessary, inconsistent, or poorly interactive.[20]

---

15 See, eg, Health and Community Services Complaints Commission (South Australia), *Submission PR 207,* 23 February 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

16 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; CrimTrac, *Submission PR 158,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

17 See, eg, Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Cancer Council Victoria, *Consultation PC 75*, Melbourne, 5 February 2007.

18 Microsoft Australia, *Submission PR 113,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

19 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

20 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

4.13 The Government of South Australia submitted that it supported 'harmonisation of privacy regimes between governments, and between the public and private sectors', but not uniform privacy laws that mirrored the *Privacy Act*.[21]

4.14 The ALRC has found that inconsistency and fragmentation in privacy regulation causes a number of problems including unjustified compliance burden and cost, impediments to information sharing and national initiatives and confusion about who to approach to make a privacy complaint. It is the ALRC's view, therefore, that national consistency should be one of the goals of privacy regulation.[22] This finding is consistent with the Senate Committee privacy inquiry and the OPC Review which both concluded that privacy laws should aim to be consistent across Australia. The Senate Committee privacy inquiry recommended that a comprehensive review of privacy regulation consider measures to ensure national consistency.[23] The OPC Review also made a number of recommendations directed to national consistency.[24]

4.15 The ALRC has adopted a flexible definition of the term 'national consistency' for the purposes of this Inquiry. For example, in some areas national consistency in the regulation of personal information requires uniformity, for example, the adoption of uniform privacy principles at the federal, state and territory level.[25] National consistency can also involve the interoperability of laws that regulate the handling of personal information, such as the harmonisation of the *Privacy Act* and the *Freedom of Information Act 1982* (Cth).[26] In other contexts, national consistency may require consistent approaches to the implementation of privacy laws and therefore require cooperation and coordination between privacy regulators.[27] In other cases, consistency in the coverage of privacy laws is the goal—for example, the removal of the small business and the employee records exemptions, or regulations for particular industries.[28]

4.16 A nationally consistent privacy regime will ensure that Australians' personal information will attract similar protection whether that personal information is being handled by an Australian Government agency or a state or territory government agency, a multinational organisation or a small business, and whether that information

---

21 Government of South Australia, *Submission PR 187,* 12 February 2007.

22 Professor Fred Cate recently stated that individuals should enjoy privacy protection that is as consistent as possible across types of data, settings, and jurisdictions: F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14.

23 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 3.

24 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 2–7.

25 See below and Ch 15.

26 See Ch 12.

27 See, eg, Ch 11 and Ch 45.

28 See Part E (Exemptions), Part G (Credit Reporting Provisions) and Part H (Health Services and Research).

is recorded in a paper file or electronically. Ensuring national consistency also will assist:

- individuals to determine what their rights are and how to enforce them;
- agencies and organisations to understand their obligations and how to comply effectively and efficiently with them; and
- regulators in managing the possible overlap of functions in some areas.[29]

4.17 The ALRC is also mindful, however, of the need for flexibility in some areas. A number of stakeholders noted that consistency of information privacy regulation across jurisdictions, between the public and private sectors, and between different kinds of business, can only be achieved if the regulation is flexible enough to accommodate the different interests, business practices, and accountabilities of those subject to the regulation.[30] The ALRC acknowledges that some sectors require specific laws when dealing with personal information, for example, the health sector, credit reporting industry and the telecommunications industry.[31]

National legislation

4.18 In IP 31, the ALRC asked what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia.[32]

4.19 One option discussed in IP 31 was national privacy legislation regulating the handling of personal information throughout Australia. Such legislation could regulate the handling of personal information in both the Australian Government public sector and the private sector. National legislation could also regulate personal information handled in the state and territory public sectors, subject to some constitutional limits. This could be achieved by amending the *Privacy Act* to clarify that the Act was intended to 'cover the field' to the exclusion of state and territory legislation. As noted in IP 31, this would raise complex political and constitutional issues.

---

29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

30 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007. See also, Centre for Law and Genetics, *Submission PR 127,* 16 January 2007 in relation to health information; and AAPT Ltd, *Submission PR 87,* 15 January 2007 in relation to telecommunications.

31 See Part H (Health Services and Research) and Part J (Telecommunications). See also the ALRC's proposals in relation to small business in Ch 35.

32 See, Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 2–1.

Constitutional issues

4.20 This section of the chapter will examine the scope of the Commonwealth's constitutional power to legislate with respect to privacy, and particularly its constitutional capacity to 'cover the field' in this area. First, it will consider various constitutional bases of power that the Commonwealth could seek to rely on for the purposes of national privacy legislation. It will then discuss the express and implied constitutional restrictions on Commonwealth legislative power.

4.21 The *Australian Constitution* includes a list of subjects about which the Australian Parliament may make laws. That list does not expressly include privacy but this does not mean that the Australian Parliament has no power in relation to privacy. The *Privacy Act* was passed on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs'.[33] The external affairs power enables the Australian Parliament to make laws with respect to matters physically external to Australia;[34] and matters relating to Australia's obligations under bona fide international treaties or agreements, or customary international law.[35] The external affairs power is not confined to meeting international obligations, but also extends to 'matters of international concern'.[36]

4.22 An important limitation on the scope of the external affairs power is that the Commonwealth Act must be an appropriate means of giving effect to the object of the relevant international treaty or agreement.[37] The Preamble to the *Privacy Act* makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the United Nations *International Convention on Civil and Political Rights*[38] (ICCPR) as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines).[39]

4.23 The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic*

---

33 *Australian Constitution* s 51(xxix). See *Privacy Act 1988* (Cth) Preamble.

34 *Horta v Commonwealth* (1994) 181 CLR 183.

35 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.

36 *Koowarta v Bjelke-Petersen* (1982) 153 CLR 168.

37 *R v Burgess; Ex parte Henry* (1936) 55 CLR 608, 646; *R v Poole; Ex Parte Henry (No 20)* (1939) 61 CLR 364; *Airlines of New South Wales v New South Wales (No 2)* (1965) 113 CLR 54, 82, 102, 118, 126, 141; *Commonwealth v Tasmania* (1983) 158 CLR 1; *Richardson v Forestry Commission* (1988) 164 CLR 261. There remains legislative discretion to choose among appropriate means for implementing those obligations: *Commonwealth v Tasmania* (1983) 158 CLR 1, 130–131.

38 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17. See discussion in Ch 1 and Ch 5.

39 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). The OECD Guidelines are discussed further in Ch 1 and Part D.

Processing of Personal Data.[40] Section 3 of the *Privacy Amendment (Private Sector) Act* makes clear that the private sector amendments were also intended to meet Australia's international obligations, as well as international concerns, relating to privacy.

4.24 In addition to the 'external affairs' power, the Commonwealth may seek to rely on other constitutional heads of power as a basis for legislating on privacy,[41] including:

- s 51(v), which empowers the Australian Parliament to make laws with respect to 'postal, telegraphic, telephonic, and other like services';[42]
- s 51(i), which empowers the Australian Parliament to make laws with respect to 'trade and commerce with other countries, and among the States'; and
- in part at least, on s 51(xx), which empowers the Australian Parliament to make laws with respect to 'foreign corporations, and trading or financial corporations formed within the limits of the Commonwealth'.[43]

4.25 National privacy legislation may also be constitutionally grounded in s 51(xiii) and (xiv) of the *Constitution* which empowers the Australian Parliament to make laws with respect to banking and insurance,[44] but not state banking or state insurance unless it extends beyond the limits of the state.

4.26 The Commonwealth may legislate so as to 'cover the field' (either expressly or impliedly) of a particular subject matter within its legislative powers.[45] The Australian Parliament could legislate in this way in relation to the handling of personal information to the exclusion of the states and territories. Such legislation, however, would be affected by the express and implied restrictions applying to all Commonwealth constitutional powers, discussed below.

Express and implied constitutional limits

4.27 As noted above, express constitutional limitations include those in ss 51(xiii) and 51(xiv) of the *Australian Constitution*, which provide that the Australian

---

40 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985).

41 Recent human rights legislation has been based on a range of constitutional powers. See, eg, *Age Discrimination Act 2004* (Cth) s 10.

42 For example, pt IIIA of the *Privacy Act* seeks to engage s 51(v) by regulating the use of 'eligible communications services' in the course of activities relevant to credit reporting. The term 'eligible communications services' is defined to mean 'a postal, telegraphic, telephonic or other like service, within the meaning of paragraph 51(v) of the *Constitution*': *Privacy Act 1988* (Cth) s 6(1).

43 The *Privacy Act* is partly directed towards the actions of 'organisations' in respect of an individual's personal information. 'Organisation' is defined to include 'a body corporate': Ibid s 6C.

44 This restriction is reflected in s 12A of the *Privacy Act* and is discussed further below.

45 *Botany Municipal Council v Federal Airports Corporation* (1992) 175 CLR 453, 464.

Parliament may legislate with respect to banking and insurance, but not state banking or state insurance that does not extend beyond the limits of the state. 'State banking' for the purposes of s 51(xiii) is the business of banking conducted within a state by a bank owned or controlled by a state.[46] Similarly, 'state insurance' bears its ordinary meaning, referring to an insurance business established and conducted by a state or its authority.[47]

4.28 In *Bourke v State Bank of New South Wales*, the High Court found that a law is a law with respect to state banking if it 'affects the actions of banks in their banking business'.[48] If the *Privacy Act* were to operate upon state banking or state insurance not extending beyond the limits of the state concerned, it would be constitutionally valid only so long as it could not be characterised as a law with respect to banking. The same rationale and outcome would apply with respect to the insurance power.

4.29 Implied constitutional limitations include the principles that a federal law may not discriminate against a state,[49] or prevent a state from continuing to exist and function as an independent unit of the federation.[50] In *Western Australia v The Commonwealth* (the *Native Title Act* Case) a majority of the High Court of Australia determined that:

> For constitutional purposes, the relevant question is not whether State powers are effectively restricted or their exercise made more complex or subjected to delaying procedures by the Commonwealth law. The relevant question is whether the Commonwealth law affects what Dixon J [in *Melbourne Corporation v The Commonwealth*] called the 'existence and nature' of the State body politic … A Commonwealth law cannot deprive the State of the personnel, property, goods and services which the State requires to exercise its powers and cannot impede or burden the State in the acquisition of what it so requires.[51]

4.30 While state powers may be 'effectively restricted or their exercise made more complex or subjected to delaying procedures' by the operation and requirements of the *Privacy Act*, the Act does not affect the existence and nature of the 'State body politic'. Therefore, it is the ALRC's view that provided that the Commonwealth acts pursuant

---

46 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 52, 65, 70, 78, 86, 97.

47 P Lane, *Lane's Commentary on The Australian Constitution* (1997), 215.

48 *Bourke v State Bank of New South Wales* (1990) 170 CLR 276, 290. The Court's decision has been subject to criticism: D Rose, 'Judicial Reasonings & Responsibilities in Constitutional Cases' (1994) 20 *Monash Law Review* 195, 199–200.

49 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 78; *Victoria v Commonwealth* (1957) 99 CLR 575; *Queensland Electricity Commission v Commonwealth* (1985) 159 CLR 192, 356; *Western Australia v Commonwealth* (1995) 183 CLR 373.

50 *Melbourne Corporation v Commonwealth* (1947) 74 CLR 31, 78; *Queensland Electricity Commission v Commonwealth* (1985) 159 CLR 192, 356; *Victoria v Commonwealth* (1971) 122 CLR 353; *Re Australian Education Union; Ex parte Victoria* (1995) 184 CLR 188.

51 *Western Australia v Commonwealth* (1995) 183 CLR 373 at 480.

to a s 51 constitutional head of power, the Commonwealth could legislate to the exclusion of the states regarding privacy in the state public and private sectors.[52]

4.31 One qualification to this may be in regards to legislative provisions applying to public sector employees in the higher levels of state government. The High Court has found that Commonwealth laws that seek to regulate state employees at the 'higher levels of government' (including ministers, ministerial assistants and advisers, heads of departments and judges) may interfere with the existence and nature of a state.[53] Another limitation may be if the *Privacy Act* purported to regulate the handling of information that goes to the core of state government functions, such as cabinet-in-confidence documents and other highly sensitive documents.

4.32 It is important to note that express and implied constitutional limitations do not apply to the territories because the Australian Parliament has plenary power to legislate in relation to them.[54] Further, Commonwealth legislation regulating the handling of personal information in the private sector to the exclusion of state legislation would not breach either the express or implied restrictions on Commonwealth power.[55]

Submissions and consultations

4.33 A large number of submissions supported comprehensive national legislation in relation to the private sector.[56] For example, the OPC submitted that:

> implementation of Australia-wide programs would be greatly assisted by overarching national standards. This could include include amending s 3 of the *Privacy Act* to clarify that the Act is intended to cover the private sector, to the exclusion of state and territory privacy legislation. With appropriate consultation, education and implementation, this may resolve many current difficulties, particularly in the private health sector.[57]

---

52 A number of pieces of federal human rights legislation, including the *Age Discrimination Act 2004* (Cth), the *Disability Discrimination Act 1992* (Cth) and the *Racial Discrimination Act 1975* (Cth), regulate the activities of state and territory public sector authorities.

53 *Re Australian Education Union; Ex parte Victoria* (1995) 184 CLR 188, 233.

54 *Australian Constitution* s 122.

55 *Re Lee; Ex parte Harper* (1986) 160 CLR 430, 453; *Western Australia v The Commonwealth* (1995) 183 CLR 373, 477.

56 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Health Insurance Association, *Submission PR 161,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; AXA, *Submission PR 119,* 15 January 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007; S Crothers, *Submission PR 43,* 14 July 2006.

57 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

4.34 The Law Council of Australia submitted that it was strongly of the view that every effort should be made to develop national privacy legislation administered by a single authority.[58]

4.35 Many submissions focused on the problems caused by overlapping federal, state and territory laws in relation to the handling of health information in the private sector. For example, Telstra submitted that:

> the operation of the *Privacy Act* should be clarified to reinforce the primacy of the national privacy regime. The introduction of State-based legislation, particularly in relation to health privacy, has resulted in additional compliance costs and an extra layer of protection that should be consolidated at a national level.[59]

4.36 A number of stakeholders suggested that the adoption of a single set of privacy principles in federal, state and territory privacy laws would assist national consistency. For example, the OPC submitted that:

> A single set of principles would be most effective where it is implemented, not only in the *Privacy Act* (to replace the IPPs and NPPs), but also in applicable state and territory legislation. This would allow for a more clear and straight-forward approach to regulating the many different sectors covered by privacy laws in Australia.[60]

4.37 Both the Queensland Government and the Government of Victoria supported the adoption of a single set of principles to regulate the Australian public sector, the private sector and state and territory public sectors.[61]

4.38 Some submissions suggested that a national law should be enacted to cover state and territory public sectors.[62] Other stakeholders submitted, however, that the states and territories should be left to regulate the handling of personal information in the public sector. For example, the Legal Aid Commission of New South Wales submitted that there are benefits in different levels of Government being able to innovate or respond to local conditions.[63] The Government of South Australia did not support national legislation regulating its public sector. It submitted that:

> Given the broad range of State and Territory law that would interrelate with any model of privacy protection, it is important that the relevant State or Territory is able to make necessary adjustments to each regime.[64]

---

58 Law Council of Australia, *Submission PR 177,* 8 February 2007.

59 Telstra, *Submission PR 185,* 9 February 2007. See also: Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007.

60 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also, eg, Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

61 Government of Victoria, *Submission PR 288,* 26 April 2007; Queensland Government, *Submission PR 242,* 15 March 2007.

62 I Turnbull, *Submission PR 82,* 12 January 2007.

63 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

64 Government of South Australia, *Submission PR 187,* 12 February 2007.

4.39 The Government of Victoria also noted that there are a number of state laws that regulate the handling of personal information by both the private sector and the state public sector, for example the *Infertility Treatment Act 1995* (Vic) and the *Adoption Act 1984* (Vic). The Government submitted that these laws typically form one critical part of the overall regulation of a particular subject matter, and cannot be divorced from, or viewed in isolation from, the general statute in which they are located.

> The Government would not support the dilution of section 3 as this may remove the ability of States and Territories to legislate for the handling of information about individuals where this is necessary to address particular policy areas administered by the State. These areas are not necessarily confined to the activities of the State public sector, but may apply to the private sector.[65]

4.40 The Australian Government Department of Health and Ageing also noted that a number of state laws would need to be preserved or incorporated into national legislation:

> Any attempt at nationally consistent legislation must consider the interaction between privacy laws and other specific legal requirements which may come directly within State or Territory responsibility, such as child protection, disability and public health.[66]

Commonwealth-state cooperative scheme

4.41 An alternative to the Australian Parliament enacting national privacy legislation is a Commonwealth-state cooperative scheme. A cooperative scheme has been defined as a scheme in which each participating jurisdiction promulgates legislation to facilitate the application of a standard set of legislative provisions in that jurisdiction to regulate a matter of common concern.[67] Commonwealth-state cooperative schemes may be categorised into three types: reference of power to the Commonwealth, mirror legislation and complementary law regimes.[68] These schemes may involve not only mirror or complementary legislation, but the cooperative use of Commonwealth or state and territory officials to administer them and to monitor compliance with them.[69]

4.42 A cooperative scheme could be used to regulate the handling of personal information in the federal and state public sectors and the private sector. Alternatively, national legislation could deal with the federal public sector and the private sector,

---

65 Government of Victoria, *Submission PR 288,* 26 April 2007. See also: Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

66 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

67 J Ledda, 'The Drafter's Guide to Cooperative Schemes' (Paper presented at Drafting Forum 2001, Melbourne) cited in M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 3.

68 Ibid, 3.

69 R French, 'Cooperative Federalism in Australia: An Intellectual Resource for Europe' (Institute of Advanced Legal Studies Public Lecture, London, 22 February 2005), 14.

while a cooperative scheme could address the handling of personal information in each of the state public sectors.

Reference to the Commonwealth

4.43 Section 51(xxxvii) of the *Australian Constitution* gives the Commonwealth Parliament power to make laws with respect to:

> matters referred to the Parliament of the Commonwealth by the Parliament or Parliaments of any State or States, but so that the law shall extend only to States by whose Parliaments the matter is referred, or which afterwards adopt the law.

4.44 The states have referred a number of matters to the Commonwealth including corporations and counter-terrorism.[70] The referral of power in relation to counter-terrorism was made on the basis that the Australian Parliament does not have a specific constitutional power to legislate in relation to terrorism. The *Security Legislation Amendment (Terrorism) Act 2002* (Cth)—which inserted a new Part 5.3 (Terrorism) into Chapter 5 of the Commonwealth *Criminal Code*—relied on a patchwork of constitutional powers. It was feared that any legal complexity or uncertainty would become the focus of litigation into the effectiveness of the new federal terrorism offences. In order to remove doubts about the extent of the Commonwealth's constitutional power, the states referred the matter under s 51(xxxvii).[71]

4.45 While the scope of the Australian Parliament's power to legislate in relation to the handling of personal information, based on the external affairs power, is wide, a referral of power by the states would ensure that federal privacy legislation was comprehensive in its coverage and less vulnerable to constitutional challenge.

Mirror legislation

4.46 Mirror legislation usually refers to a system where one jurisdiction enacts a law that is then enacted in similar terms by other jurisdictions.[72] An example of mirror legislation is the fair trading legislation contained in the *Trade Practices Act 1975* (Cth). Each Australian state and territory has passed legislation that largely mirrors the consumer protection provisions of Divisions 1 and 1A of Part V of the *Trade Practices Act.*

---

70 See, eg, *Workplace Relations Act 1996* (Cth) pt XV; *Commonwealth Powers (Industrial Relations) Act 1996* (Vic); *Criminal Code Act 1995* (Cth) pt 5.3; *Terrorism (Commonwealth Powers) Act 2003* (Vic). The *Corporations Act 2001* (Cth) is based, in part, on reference of matters by the states to the Commonwealth. The decision to adopt such references was influenced by a number of successful challenges to the Commonwealth's attempts to develop uniform corporations law: see *R v Hughes* (2000) 171 ALR 155; *Re Wakim; ex parte McNally* (1999) 198 CLR 511. A reference to the Commonwealth would not be required from the ACT, the Northern Territory and Norfolk Island because s 122 of the *Australian Constitution* assigns to the Commonwealth the power to 'make laws for the government' of the territories.

71 Explanatory Memorandum, Terrorism (Commonwealth Powers) Bill 2003 (Vic).

72 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 4–5.

4.47 Each Australian state could pass similar legislation to regulate the handling of personal information by the private sector, or that state's public sector. Mirror legislation can result in inconsistency, however, both at the time the legislation is enacted and as laws are amended.[73] One option for dealing with this is to have a central body to maintain uniformity.[74]

Complementary law regime

4.48 A complementary applied law scheme involves one jurisdiction (which need not be the Commonwealth) enacting a law on a topic, which is then applied by other jurisdictions.[75] Where the Australian Parliament enacts a law that applies to specified matters within Commonwealth constitutional power, the law will apply in the states as a Commonwealth law to the extent possible. State legislation will apply to the extent that its application is consistent with the application of the Commonwealth law.[76]

> In the perfect applied law regime where a law is promulgated by one jurisdiction and is picked up by other jurisdictions as in force from time to time, there are effective limits (which may be non-legislative) on modification and there is central administration and enforcement of that law, which can be expected to provide a substantial degree of uniformity.[77]

4.49 Uniformity can be reduced, however, if an applied law regime does not involve central administration. Further, any capacity for the applying state to have control over the text of the legislation can also lead to inconsistency.[78]

4.50 An example of a complementary applied law scheme is the agricultural and veterinary chemicals legislation under the *Agricultural and Veterinary Chemicals Code Act 1994* (Cth). The Australian Parliament enacted the *Agricultural and Veterinary Chemicals Code* to apply to 'participating territories' and with provisions to enable the states to apply the text of the Code as a law of the state. All states and territories have adopted the Code in relevant legislation. The Act confers regulatory functions on the National Registration Authority for Agricultural and Veterinary Chemicals, establishing it as the national authority responsible for the evaluation, registration and review of agricultural and veterinary chemicals and their control up to their point of sale. The states and territories retain responsibility for control-of-use activities, such as licensing of pest control, operators and aerial spraying. Some states have also enacted

---

73 See, eg, Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Harmonisation of Legal Systems within Australia and between Australia and New Zealand* (2006), [2.26]; Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 1.

74 See, eg, Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Rec 2–1.

75 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 8.

76 Ibid, 9.

77 Ibid, 10.

78 Ibid, 10.

legislation relating to the enforcement of the Code. For example, the *Agricultural and Veterinary Chemicals (Control of Use) Act 1995* (Tas) establishes the Agricultural, Silvicultural and Veterinary Chemical Council.

4.51 The *Competition Code* under the *Trade Practices Act 1975* (Cth) is another example of a complementary applied law regime.[79] An issue that challenges national consistency in relation to the *Competition Code* is a state's ability not to apply a Commonwealth amendment to the Code within their jurisdiction. For example, s 6 of the *Competition Policy Reform (Queensland) Act 1996* (Qld) enables the Queensland Parliament to pass a regulation declaring that a Commonwealth amendment does not apply in the state. Section 150K of the *Trade Practices Act 1974* (Cth), however, enables the Commonwealth Minister to prevent a state from enacting a law that provides an exemption from the Act.

4.52 One option would be for the Australian Parliament to enact legislation dealing with the handling of personal information by the Australian Government public sector and private sector. This legislation would include the proposed Unified Privacy Principles, and the proposed *Privacy (Health Information) Regulations* as in force under the *Privacy Act*. The Unified Privacy Principles and the *Privacy (Health Information) Regulations* could then be adopted by the states in legislation to apply to state and territory public sectors as in force under the *Privacy Act* from time to time.

4.53 A complementary (non-applied) law scheme has been adopted in relation to the classification of films, publications and computer games. Films, publications and computer games are classified under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) while the controls and penalties are imposed under state and territory legislation.[80] One option would be for the Australian Parliament to enact laws establishing a set of privacy principles, and for the states and territories to enact legislation to enforce compliance.

Combined scheme

4.54 Another model is a scheme that combines mirror legislation and applied law approaches. In this model, some states could enact their own law mirroring federal laws that regulate personal information and other states could apply the Commonwealth law as a law of the state. Examples of this approach include the therapeutic goods and gene technology regulatory schemes.

4.55 The *Gene Technology Act 2000* (Cth) extends to matters within the Commonwealth's power, leaving the states with the option of either applying the

---

79 See *Trade Practices Act 1974* (Cth) pt XIA.

80 See, eg, *Classification (Publications, Films and Computer Games) Enforcement Act 1995* (Vic). The *Classification (Publications, Films and Computer Games) Act 1995* (Cth) was recently amended to provide for, among other things, integration of the Office of Film and Literature Classification into the Attorney-General's Department: *Classification (Publications, Films and Computer Games) Amendment Act 2007* (Cth).

federal Act or enacting their own legislation. Both options have been adopted by different states. For example, NSW has opted for the applied law model while Victoria has adopted mirror legislation.[81] Section 26 of the *Gene Technology Act 2000* (Cth) establishes the independent position of the Gene Technology Regulator. The Regulator oversees the accreditation of research facilities and licences experimental and commercial dealings.[82]

4.56 Some commentators have suggested that national consistency of the gene technology scheme is being undermined by the states having inconsistent approaches to the issuing of moratoriums on the commercial release of genetically modified organisms.[83] A recent statutory review recommended that all jurisdictions should reaffirm their commitment to a nationally consistent scheme, including a nationally consistent approach to market considerations, and work together to develop a national co-existence framework.[84]

Submissions and consultations

4.57 A large number of submissions were supportive of a cooperative scheme, noting that the regulation of personal information should not be left to the Commonwealth.[85] For example, the OPC submitted that ensuring that privacy protections in state and territory jurisdictions are consistent with, and at least equivalent to, the *Privacy Act* would assist national consistency. It noted that for the purposes of introducing uniform privacy principles across both Commonwealth and state and territory public sectors, a cooperative scheme between the Australian Government and the states may provide the best avenue.

> An ideal outcome would be for the states to have input into the development of a uniform set of principles for the *Privacy Act* and then amend their own privacy legislation to enact the agreed upon principles.[86]

4.58 The Office of the Information Commissioner Northern Territory submitted that:

> The obvious merits of adopting a consistent approach to privacy protection should not prevent states and territories from making decisions about what best suits their constituents. Any move to general consistency should recognise that particular aspects

---

81 See *Gene Technology (NSW) Act 2003* (NSW) and the *Gene Technology Act 2001* (Vic).

82 The *Intergovernmental Agreement on Gene Technology* is discussed further below.

83 See M Tranter 'A Question of Confidence: An Appraisal of the Operation of the *Gene Technology Act 2000*' (2003) 20(4) *Environmental and Planning Law Journal* 10; C McGrath 'A System Under Strain: The Regulation of Gene Technology' (2003) 2 *National Environmental Law Review* 32.

84 Australian Government Department of Health and Ageing, *Statutory Review of the Gene Technology Act 2000 and the Gene Technology Agreement* (2006), rec 9.1.

85 See, eg, Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

86 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

> of the scheme may be modified if it is considered necessary by a particular jurisdiction.[87]

4.59 While a reference of power to the Commonwealth under s 51(xxxvii) of the *Australian Constitution* has a number of advantages in terms of constitutional validity and national consistency, there was very little support for this model in submissions.[88] For example, the Office of the Victorian Privacy Commissioner (OVPC) stated that this model would remove the state's ability to provide enhanced protection and raised issues of interaction with state-based freedom of information, archives and human rights laws.[89] The Australian Privacy Foundation submitted that it would not be desirable to have a referral of powers, emphasising the importance of having a local regulator to handle complaints, and provide advice and training programs.[90]

4.60 A number of submissions and consultations supported mirror legislation.[91] For example, the Queensland Government submitted that a consistent set of privacy principles binding both public and private sectors should be adopted by each jurisdiction by way of mirror legislation. Each jurisdiction would then be responsible for administering the relevant legislation, for establishing and maintaining complaint resolution mechanisms, undertaking advocacy, education and awareness activities and monitoring the operation of the scheme.[92]

4.61 The Government of South Australia preferred a complementary cooperative scheme, whether legislatively applied or not, where the Commonwealth has responsibility for the private sector and the Australian Government, and the states and territories have responsibility for state and local government and universities.[93]

4.62 The Government of Victoria stated that its preferred model is an applied law model because it has the advantage of rating highly on 'federal values' whilst still ensuring a very high level of uniformity, making it an appropriate model for harmonising privacy principles. The Government noted that if such a model were adopted in relation to privacy regulation, it could be underpinned by an intergovernmental agreement that provides for the following:

> - Commonwealth legislation establishing nationally agreed and binding privacy principles for its own public sector based on principles adapted from the NPPs;
>
> - legislation establishing the same privacy principles for the private sector (presumably Commonwealth legislation covering all jurisdictions,

87 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
88 M Fenotti, *Submission PR 86,* 15 January 2007 was an exception.
89 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
90 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
91 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
92 Queensland Government, *Submission PR 242,* 15 March 2007.
93 Government of South Australia, *Submission PR 187,* 12 February 2007.

> although other options would be possible such as State legislation automatically applying the same principles to their own private sector if all jurisdictions agreed to do this);
>
> - State and Territory legislation adopts and automatically applies the privacy principles to their respective public sectors (that is, incorporating them by reference, not repeating the principles in their own legislation), and applying that law as it is set out in the Commonwealth Act from time to time. The intergovernmental agreement would provide that the Commonwealth Act would only be amended per the process outlined below;
>
> - a national process for reaching agreement about alterations to the privacy principles which would require the approval of a ministerial council or another intergovernmental process. This would ensure that the scheme remains a truly co-operative one, that would take into account the experiences of all jurisdictions;
>
> - an agreed statutory complaints handling process, generally involving local resolution of complaints using locally based privacy regulators and access to remedies within the jurisdiction.[94]

4.63 Electronic Frontiers Australia Inc was opposed to a complementary non-applied scheme such as that adopted in relation to the classification of films, publications and computer games. It was said that such a model enables a single jurisdiction to prevent changes to the legislation, notwithstanding overwhelming support from the public and other jurisdictions' governments for change.[95]

A model for national consistency

National legislation

4.64 The problems associated with overlapping and inconsistent federal, state and territory laws that regulate the handling of personal information are documented throughout this Discussion Paper. These problems include unjustified compliance burden and cost, impediments to information sharing and national initiatives and confusion about who to approach to make a privacy complaint. It is the ALRC's view that the most appropriate method of responding to these problems is the enactment of federal legislation to regulate the handling of personal information, to the exclusion of state and territory privacy laws, subject to a qualification discussed below in relation to state and territory public sectors.

4.65 As noted above, it is the ALRC's view that the Australian Parliament has the power under the *Australian Constitution* to legislate to the exclusion of the states regarding privacy in the state public and private sectors. The only qualification to this may be in regards to legislative provisions applying to state banking and state

---

94 Government of Victoria, *Submission PR 288,* 26 April 2007.

95 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

insurance that does not extend beyond the limits of the state, public sector employees in the higher levels of state government, and information that goes to the core of state government functions, such as cabinet-in-confidence documents.

4.66 The ALRC notes, however, the concerns raised by state governments and others that the states and territories should be left to regulate the handling of personal information in the public sector. In particular, the ALRC notes concerns relating to the need for state and territory privacy legislation to respond to local conditions, and to interact with existing state and territory information laws such as freedom of information and public records legislation. Further, the ALRC acknowledges the advantages of having state and territory privacy regulators to deal with complaints, provide advice, and perform educational functions.

4.67 While the *Privacy Act* could accommodate many of these concerns, the ALRC's view is that, for the time being, the Australian Parliament should only exercise its legislative power in relation to the handling of personal information by the private sector. The ALRC proposes below a Commonwealth-state cooperative scheme in relation to state and territory public sectors.

4.68 The problems associated with overlapping federal, state and territory laws that regulate the handling of personal information in the private sector are detailed in Chapter 11 and Part H of this Discussion Paper. A large number of submissions focused on inconsistency in the regulation of personal health information. Submissions suggested that various problems arise because the handling of health information in the private sector is regulated by the *Privacy Act* and state and territory legislation in NSW, Victoria and the ACT.[96]

4.69 Submissions noted that these laws are creating a significant compliance burden and cost, and are preventing the implementation of projects that are in the public interest, such as medical research. In addition, health consumers in those jurisdictions are faced with two sets of principles and two possible avenues of complaint. These submissions urged the ALRC to propose the enactment of national privacy laws that regulate the handling of health information.

4.70 It is the ALRC's view that these issues would be effectively dealt with if organisations were required to comply with a single set of principles in relation to the handling of health information. In the 2003 report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and AHEC recommended that:

> As a matter of high priority, the Commonwealth, States and Territories should pursue the harmonisation of information and health privacy legislation as it relates to human

96 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

> genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.[97]

4.71 The ALRC proposes that the *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by the private sector. In particular, the following laws of a state or territory should be excluded to the extent that they apply to organisations: *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); and the *Health Records (Privacy and Access) Act 1997* (ACT).

4.72 The ALRC notes that other state and territory laws may be introduced that seek to regulate the handling of personal information in the private sector. The ALRC has therefore proposed that regulations made under the *Privacy Act* should operate to exclude laws that regulate the handling of personal information by organisations. For example, the Information Privacy Bill 2007 (WA) proposes to regulate the handling of health information by the private sector in Western Australia. Further, the *Information Privacy Act 2000* (Vic) could potentially regulate the handling of personal information by private sector organisations that are declared to be 'organisations' for the purposes of the Act.[98] It is the ALRC's view that the *Privacy Act* should operate to exclude the operation of such laws.

4.73 A number of federal laws include provisions that state the Commonwealth's intention to 'cover the field'. Section 16(1) of the *Workplace Relations Act 1996* (Cth) states that the Act is intended to apply to the exclusion of a number of listed laws of a state and territory so far as they would otherwise apply in relation to an 'employee' or 'employer'.[99] The ALRC has adopted this provision as a model for its proposal to exclude the operation of state and territory laws dealing with the handling of personal information by organisations.

4.74 The ALRC also proposes that states and territories with information privacy legislation that purports to apply to private sector organisations, should amend that legislation so that it is no longer expressed to apply to private sector organisations.

---

97 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–1.

98 *Information Privacy Act 2000* (Vic) s 9.

99 Another model is *Corporations Act 2001* (Cth) pt 1.1A.

Proposal 4–1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic);

(c) *Health Records (Privacy and Access) Act 1997* (ACT); and

(d) any other laws prescribed in the regulations.

Proposal 4–2 States and territories with information privacy legislation that purports to apply to private sector organisations should amend that legislation so that it is no longer expressed to apply to private sector organisations.

4.75 As noted above, submissions from state and territory governments and others noted that there are various state and territory laws that regulate the handling of personal information in the private sector that would need to be preserved if the Australian Government enacted national privacy legislation. These laws include state and territory laws that require reporting for public health purposes and reporting for child protection purposes.

4.76 It is the ALRC's view that there are good public interest reasons why these state and territory laws should be preserved under national privacy legislation. For example, state and territory public health Acts require health service providers (including health service providers in the private sector) to collect and record certain information about health consumers with 'notifiable diseases', such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[100] Other state and territory laws contain provisions that require mandatory reporting when a child is suspected of being at risk of harm.[101] These provisions usually apply to persons who work in areas such as health care, welfare, education, children's services, residential services, or law enforcement in both the public and private sectors.

4.77 In Chapter 11, the ALRC notes that some state and territory legislation does not include provisions in relation to contracted service providers. Stakeholders have

100 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

101 See , eg, *Children, Youth and Families Act 2005* (Vic) pt 4.4; *Child Protection Act 1999* (Qld); *Children's Protection Act 1993* (SA) pt 4; *Children Young Persons and Their Families Act 1997* (Tas) pt 3.

expressed concern that this results in some organisations that contract with state and territory governments, in particular small businesses, being unregulated by privacy legislation. The ALRC therefore proposes that state and territory legislation should include provisions that regulate the handling of personal information by organisations when contracting with state and territory government agencies.[102] These laws would also need to be preserved by national legislation that regulates personal information by the private sector to the exclusion of the states and territories.

4.78 While the proposed Unified Privacy Principles would accommodate most of these laws,[103] to ensure clarity the ALRC proposes that the *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the legislation. Section 16 of the *Workplace Relations Act 1996* (Cth), for example, provides that the Act operates to the exclusion of state and territory law, except in relation to a list of 'non-excluded matters'. The non-excluded matters are broad categories of laws such as 'superannuation', 'long service leave' and 'child labour'. The ALRC has adopted this provision as a model to deal with state and territory laws that should be preserved under the *Privacy Act*.

4.79 The ALRC has been advised of a range of other state and territory laws that regulate the handling of personal information in the private sector that should be preserved under national privacy laws. These laws include laws regulating adoption, infertility treatment, disability service providers, and health services.[104] The ALRC has not undertaken a comprehensive review of all state and territory laws that regulate the handling of personal information. It is the ALRC's view, however, that it is vital that the Australian Government should consult with state and territory governments about what groups of laws should be preserved under an extended *Privacy Act*. The ALRC proposes that the Australian Government, in consultation with state and territory governments, should develop a list of 'non-excluded matters' for the purposes of the *Privacy Act*.

Proposal 4–3 The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the legislation. The Australian Government, in consultation with state and territory governments, should develop a list of 'non-excluded matters', for example matters such as:

(a) reporting for child protection purposes;

---

102 See Proposal 4–4 below.

103 Such as the exception to the proposed 'Use and Disclosure' principle in the Unified Privacy Principles for uses and disclosures that are 'required or authorised by or under a law'.

104 See, eg, Government of Victoria, *Submission PR 288,* 26 April 2007, Attachment A.

(b) reporting for public health purposes; and

(c) the handling of personal information by state and territory government contractors.

A Commonwealth-state cooperative scheme

4.80 It is the ALRC's view that national consistency will be promoted if the Commonwealth, and state and territory governments enter into an intergovernmental agreement in relation to the handling of personal information. The intergovernmental agreement should establish a Commonwealth-state cooperative scheme that provides that the states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector.

4.81 The ALRC has not proposed that the states and territories develop legislation that mirrors the *Privacy Act*. As noted above, it is the ALRC's view that the states and territories should develop their own legislation that can accommodate existing state and territory information laws and complaint and enforcement mechanisms. State and territory legislation should apply the privacy principles under the *Privacy Act* and should, at a minimum, adopt certain provisions of the *Privacy Act*.

4.82 A major cause of inconsistency in Australian privacy laws is that the *Privacy Act* and state and territory privacy laws include similar, but not identical, privacy principles. In the ALRC's view, the most effective method of dealing with these inconsistencies is the adoption of identical privacy principles at the federal, and state and territory level. The ALRC therefore proposes that the intergovernmental agreement establishing the Commonwealth-state cooperative scheme should provide that state and territory legislation should apply the proposed Unified Privacy Principles and the proposed *Privacy (Health Information) Regulations* as in force under the *Privacy Act* from time to time. The ALRC notes the success of other applied law schemes in achieving national consistency, including the agricultural and veterinary chemical legislation, the *Competition Code*, and gene technology laws.

4.83 The various problems caused by the use of inconsistent terms and definitions across federal information laws are outlined in Chapter 12. As noted in Chapter 14, definitions of key terms used in state and territory privacy laws generally conform to those used under the *Privacy Act*. However, there are some differences. In the ALRC's view, relevant definitions of key terms used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information') should be adopted in state and territory laws that regulate the handling of personal information in the public sector.[105]

105 Proposed definitions of these terms are discussed in Ch 3 and Ch 57.

4.84 Chapter 11 examines how inconsistency in federal, state and territory privacy laws acts as an impediment to appropriate information sharing across state borders. It is the ALRC's view that, rather than preventing appropriate information sharing, privacy laws and regulators should encourage public sector agencies and private sector organisations to design information sharing schemes that are compliant with privacy requirements or, where necessary, seek suitable exemptions or changes to legislation to facilitate information sharing projects.

4.85 In the ALRC's view, an effective way to facilitate information sharing between Australian Government agencies, state and territory agencies and the private sector is the adoption of the *Privacy Act* provisions that allow public interest determinations and temporary public interest determinations in state and territory laws regulating the public sectors. This proposal will allow state and territory agencies to share information with Australian Government agencies and organisations when it is in the public interest, but would otherwise be prevented under that state's or territory's privacy laws.

4.86 Inconsistencies between the *Privacy Act* and state and territory privacy laws have resulted in regulatory gaps in relation to state and territory incorporated bodies (including statutory corporations) in some jurisdictions.[106] State and territory laws that regulate the handling of personal information in that state or territory's public sector should include provisions relating to state and territory incorporated bodies (including statutory corporations). In the event that the states and territories do not enact such provisions, the ALRC has proposed that the *Privacy Act* will apply to statutory corporations in that jurisdiction.[107]

4.87 In Chapter 11, the ALRC notes that some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state or territory privacy principles for the purposes of the contract. Other state regimes provide that compliance with the state privacy regime is subject to any outsourcing arrangements, or are silent on this issue. A number of concerns were raised in submissions that organisations that contracted with state governments, in particular, small business, remain unregulated by privacy legislation. The ALRC therefore proposes that state and territory legislation regulating the handling of personal information in that state or territory's public sector should include provisions relating to state and territory government contracts.

4.88 In Chapter 47, the ALRC proposes the adoption of a data breach notification requirement. It is the ALRC's view that an agency (including a state or territory agency) should be required to notify the relevant regulator and any affected individuals when a data breach poses a real risk of serious harm to any affected individuals. The

106 See Ch 14.
107 See Ch 34.

ALRC notes the various benefits of this requirement, and the problems caused by an inconsistent approach to this requirement in the United States.[108]

Proposal 4–4 The states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector that:

(a) applies the proposed Unified Privacy Principles (UPPs) and the proposed *Privacy (Health Information) Regulations* as in force under the *Privacy Act* from time to time; and

(b) includes at a minimum:

(i) relevant definitions used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information');

(ii) provisions allowing public interest determinations and temporary public interest determinations;

(iii) provisions relating to state and territory incorporated bodies (including statutory corporations);

(iv) provisions relating to state and territory government contracts; and

(v) provisions relating to data breach notification.

The legislation also should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

Other options

4.89 In IP 31, the ALRC considered whether national legislation should set out minimum standards for the protection of personal information in state and territory public sectors, but allow those provisions to 'roll back' once a state or territory enacts laws that conform to specified federal minimum standards. There are examples of rollback provisions in various federal laws.[109] An example of this kind of scheme is s 26(2)(b) of the *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act). That section provides that the Governor-in-Council may, by order, exempt an organisation, activity or class of organisations or activities from the

108 See discussion in Ch 47.

109 *Gene Technology Act 2000* (Cth) s 14; *Environmental Protection (Sea Dumping) Act 1981* (Cth) s 9.

application of the Act if satisfied that legislation of a province that is 'substantially similar' to the PIPED Act applies to that organisation.

4.90 The Australian Privacy Foundation submitted that the federal, state and territory governments should each be directly responsible and accountable for the decisions they make concerning the information they collect from the public. It would support, however, interim provisions in a federal law that could apply to the jurisdictions that do not yet have a privacy law and which could be 'rolled back' upon the introduction of a local equivalent law.[110] The OVPC also supported such a proposal provided it allowed for higher protection to be adopted by the state and territory governments.[111]

4.91 The ALRC has not proposed that a 'roll back' provision should operate generally in relation to state and territory agencies. It has proposed, however, the use of such a mechanism in relation to state statutory corporations, and state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).[112]

4.92 The ALRC also notes s 6F of the *Privacy Act* allows the Act to be extended to cover the handling of personal information by state and territory instrumentalities at the initiative of the states and territories. The OVPC submitted that s 6F of the *Privacy Act* should be retained in its current form.

> While it appears not to have been used, it may be in the future and this type of mechanism maintains control by and independence of the states.[113]

4.93 The ALRC agrees that s 6F is a useful mechanism to bring state and territory bodies under the operation of the *Privacy Act* and should be retained in the Act.

A review

4.94 The Australian Parliament has the power under the *Australian Constitution* to legislate to the exclusion of the states regarding privacy in the state public and private sectors, subject to some limitations.[114] The ALRC considers, however, that for the time being the states and territories should participate in a Commonwealth-state scheme that provides for state and territory laws to regulate the handling of personal information in state and territory public sectors.

4.95 Given the importance of national consistency, as discussed above, it is the ALRC's view that the Australian Government should initiate a review in five years

---

110 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
111 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
112 See Chs 34 and 13 respectively.
113 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
114 See discussion of 'Constitutional issues' above.

time to consider whether the participation in the proposed Commonwealth-state scheme in relation to the handling of personal information in state and territory public sectors has achieved its goal. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors.

Proposal 4–5 The Australian Government should initiate a review in five years to consider whether the proposed Commonwealth-state cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors.

A permanent standing body

4.96 The OPC Review suggested that if national consistency is to be achieved there needs to be greater cooperation between the Australian and state and territory governments in developing legislation that has privacy implications.[115] The Australian Information Industry Association submitted to the OPC Review that the Australian Government needs to take the lead to ensure that disparate policies do not emerge.[116] The Insurance Council of Australia submitted that:

> Federal and State Ministers should work together to ensure that privacy regulation is developed in a coherent and consistent manner. Health ministers should promote co-ordination between the States in the development of privacy legislation.[117]

4.97 The health sector has in place a process for ensuring ongoing Australian and state and territory government cooperation in the area of health privacy. The National Health Privacy Working Group of the Australian Health Ministers' Advisory Council (AHMAC) has developed a draft *National Health Privacy Code*.[118] Further, the Australian Government has announced that SCAG has agreed to establish a working group to advise Ministers on options for improving consistency in privacy regulation.[119]

---

115 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 43.

116 Australian Information Industry Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004, 1.

117 Insurance Council of Australia, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004, 4.

118 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003).

119 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 26.

4.98 In IP 31, the ALRC discussed the establishment of a permanent standing body to ensure national consistency in the regulation of personal information. Such a proposal raises a number of issues including: the membership of such a body, its functions and powers, who the body would be required to report to, and resourcing.

Options for reform

4.99 One option for consideration is to broaden the membership and functions of the Privacy Advisory Committee established under the *Privacy Act*.[120] Another option would be for a ministerial council to perform such a function. A ministerial council is generally made up of ministers of all Australian states and territories, and the Commonwealth who meet to discuss matters of mutual interest.

4.100 COAG is the peak intergovernmental forum in Australia. COAG comprises the Prime Minister, state premiers, territory chief ministers and the President of the Australian Local Government Association (ALGA). The COAG Secretariat is located within the Department of the Prime Minister and Cabinet. The role of COAG is to initiate, develop and monitor the implementation of policy reforms that are of national significance and which require cooperative action by Australian governments.

4.101 The Standing Committee of Attorneys-General (SCAG) is a national ministerial council. Its members are the Australian Attorney-General and Minister for Justice and Customs, the state and territory attorneys-general and the New Zealand Attorney-General. Norfolk Island has observer status at SCAG meetings. SCAG seeks to achieve uniform or harmonised action within the portfolio responsibilities of its members. The types of issues that SCAG considers can be quite varied. An item is likely to be appropriate for SCAG if it:

- requires joint action from the Australian, state and territory governments;
- involves the development of model or uniform model legislation; or
- is of relevance to attorneys-general.[121]

4.102 SCAG has considered privacy issues related to residential tenancy databases,[122] and is currently consulting stakeholders about potential options for reform in the area of workplace privacy. SCAG also has oversight of a cooperative scheme—the National Classification Scheme for film and video and for printed material. The

120 The Privacy Advisory Committee is discussed in Ch 43.

121 Australian Government Attorney-General's Department, *Standing Committee of Attorneys-General* <www.ag.gov.au> at 30 July 2007.

122 See Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

Intergovernmental Agreement on Censorship requires that certain changes to the National Classification Scheme must be considered and agreed to by all ministers.

4.103 Another example of a ministerial council model is the Gene Technology Ministerial Council (GTMC). The GTMC oversees the implementation of the *Gene Technology Act 2000* (Cth) and the Gene Technology Regulator. The GTMC was established by an intergovernmental agreement between the Australian Government and all state and territory governments. The intergovernmental agreement also commits state and territory governments to enact corresponding state and territory legislation.[123]

4.104 The functions conferred upon the GTMC by the intergovernmental agreement include: issuing policy principles, policy guidelines and codes of practice to govern the activities of the Regulator and the operation of the scheme; approve the appointment (and, if necessary, the dismissal) of the Regulator; and consider and, if thought fit, agree on proposed changes to the scheme.[124] The GTMC is supported by the Gene Technology Standing Committee comprised of senior Commonwealth and state department officials, and the Regulator is supported by the Office of the Gene Technology Regulator.

Submissions

4.105 Only a few submissions addressed the option of a permanent standing body. Of those submissions, the majority supported a body to ensure national consistency in the regulation of personal information. In most cases, such a body was supported as a means of ensuring consistency in a Commonwealth-state cooperative scheme such as mirror legislation or applied legislation.

4.106 Most submissions addressing this issue supported a ministerial council model. For example, the Centre for Law and Genetics suggested a ministerial council model similar to that used in the gene technology regulatory scheme.[125] The Government of Victoria proposed:

> a national process for reaching agreement about alterations to the privacy principles which would require the approval of a ministerial council or another intergovernmental process. This would ensure that the scheme remains a truly co-operative one, that would take into account the experiences of all jurisdictions … A similar model would apply in relation to nationally agreed health privacy principles, which are currently being progressed through the Australian Health Ministers' Conference (AHMC).[126]

4.107 Privacy NSW submitted that it is important that a coordinating body such as SCAG maintain a supervisory role over any national scheme for privacy regulation.[127]

---

123 The *Intergovernmental Agreement on Gene Technology*, cl 9.
124 Ibid, cl 9.
125 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
126 Government of Victoria, *Submission PR 288,* 26 April 2007.
127 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

Some stakeholders in consultation meetings questioned whether SCAG or COAG would be the appropriate bodies. On the other hand, it was noted that the COAG and SCAG processes are time consuming, but that where there is the political will, the process can work effectively.

4.108 The Queensland Government's preferred model for a permanent standing body involves a national standing committee of privacy representatives selected by constituent governments to assess and endorse proposals for future reform and amendment of the privacy principles.[128] The OVPC submitted that there is some merit in the creation of a permanent standing body comprising all jurisdictions' privacy commissioners to consider and promote national consistency, information sharing between regulators, cooperative arrangements for enforcement, and enhanced legislative scrutiny of bills that may adversely impact on privacy.[129]

4.109 The Australian Privacy Foundation did not support the establishment of a permanent standing body on privacy. The Foundation submitted that such bodies have 'delayed or buried privacy issues in the past'.

> The Issues Paper mentions the Health Privacy Working Group of the Australian Health Ministers' Advisory Council, which is a poor example. It has failed after many years to produce a national health privacy code, the most recent public draft of which was released in 2003. The Standing Committee of Attorneys General has similarly been unsuccessful in tacking national privacy issues.[130]

ALRC's view

4.110 The ALRC considers that a permanent standing body will assist in maintaining national consistency in the regulation of personal information. As noted above, it is the ALRC's view that national consistency will be promoted if the Commonwealth, state and territory governments enter into an intergovernmental agreement to establish a cooperative scheme in relation to the regulation of personal information. The intergovernmental agreement should provide that any proposed changes to the proposed:

- Unified Privacy Principles must be approved by SCAG; and
- *Privacy (Health Information) Regulations* must be approved by SCAG, in consultation with the Australian Health Ministers' Advisory Council (AHMAC).

4.111 The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the

---

128 Queensland Government, *Submission PR 242,* 15 March 2007.
129 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
130 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

4.112 It is the ALRC's view that SCAG is the most appropriate body to ensure national consistency as it is an established body that has experience in considering privacy issues and in promoting consistency through cooperative schemes. One issue is that, while the majority of state and territory ministers with responsibility for the regulation of personal information are Attorneys General, the Minister responsible for information privacy in South Australia is not.[131] However, SCAG has adopted procedures to accommodate this situation in its oversight of the National Classification Scheme. SCAG procedures provide that where in any jurisdiction the Minister responsible for censorship is not the Attorney-General, that Minister attends for discussion of censorship matters. When considering any changes to the *Privacy (Health Information) Regulations*, SCAG must consult with the Australian Health Ministers' Advisory Council (AHMAC).

4.113 To ensure that all views are taken into account when issues relating to the unified privacy principles and *Privacy (Health Information) Regulations* arise, the ALRC has proposed that the amendment process should be informed by the advice of an expert advisory committee established to assist SCAG. The committee should comprise representatives from state and territory bodies with responsibility for privacy, as well as others with an interest in privacy issues. The Advisory Committee established by the ALRC for the purposes of this Inquiry provides a workable model. The Committee could address issues related to national consistency such as information sharing between privacy regulators, cooperative arrangements for enforcement, and enhanced legislative scrutiny of federal, state and territory bills that may adversely impact on national consistency in the regulation of personal information.

Proposal 4–6 To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the proposed:

(a) UPPs must be approved by SCAG; and

(b) *Privacy (Health Information) Regulations* must be approved by SCAG, in consultation with the Australian Health Ministers' Advisory Council (AHMAC).

131 The Minister responsible for information privacy in South Australia is currently the Minister for Finance.

The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

Proposal 4–7 The Standing Committee of Attorneys-General should be assisted by an expert advisory committee to:

(a) provide advice in relation to the amendment of the proposed UPPs and *Privacy (Health Information) Regulations*;

(b) address issues related to national consistency such as the scrutiny of federal, state and territory bills that may adversely impact on national consistency in the regulation of personal information; and

(c) address issues related to the enforcement of privacy laws, including information sharing between privacy regulators and cooperative arrangements for enforcement.

Appointments to the expert advisory committee should ensure a balanced and broad-based range of expertise, experience and perspectives relevant to the regulation of personal information. The appointments process should involve consultation with state and territory governments, business, privacy and consumer advocates and other stakeholders.

A single privacy regulator?

4.114 As noted in Chapter 11, a number of issues may arise because more than one body is responsible for the regulation of personal information. In Australia there are multiple privacy regulators in particular industry sectors as well as across jurisdictions. In IP 31, the ALRC noted that one issue for consideration is whether all formal complaints about privacy should be dealt with by the Privacy Commissioner, rather than by industry ombudsmen and other federal, state and territory regulators. Another option is that all formal complaints about privacy under federal legislation could be referred to the Privacy Commissioner. Alternatively, the various regimes governing the regulation of privacy at the federal, state and territory levels could be amended to clarify the jurisdiction of each of the bodies that regulate the handling of personal information.

Submissions

4.115 The ALRC did not receive many submissions on this issue. A number of stakeholders, however, vigorously opposed a body, such as the OPC, regulating state and territory public sectors.

4.116 The Government of South Australia submitted that it would not accept

> Commonwealth law directly regulating its public sector, in particular, any proposal that the Commonwealth Privacy Commissioner exercises powers of entry, search and examination in respect of State or Territory Governments. Other models discussed in the Issues Paper, such as complementary laws, are preferable.[132]

4.117 The Government of Victoria submitted that local accessible complaints resolution and remedies through state-based commissioners should be preserved. The OVPC noted that having a comprehensive national privacy law can impact negatively on enforcement and other functions associated with privacy regulation if regulation is to be the sole province of a single national office by:

- reducing the field for public comment on privacy issues of multi- or cross-jurisdictional concern;
- eliminating an avenue for state bodies to seek advice on potential adverse privacy impact, if a state body is not empowered or available to provide advice (including on cabinet-in-confidence matters and sensitive pilot and other projects);
- reducing individuals' ability to access justice in making complaints locally and seeking redress, if having to rely on a national regulator; and
- minimising the ability to conduct audits and investigations into privacy sensitive acts and practices.

4.118 The OVPC submitted that maintaining and promoting a national framework for having privacy laws and regulators in each jurisdiction fosters greater access to justice by those seeking redress, enables advice to be provided by offices that have developed local expertise, and allows for compliance actions to be undertaken in response to issues and concerns that arise within particular jurisdictions. The OVPC noted that there is more likely to be resourcing problems for handling complaints and generating awareness, and a lack of expertise in other relevant state and territory laws, if national legislation was to establish a single national privacy regulator.[133]

---

132 Government of South Australia, *Submission PR 187,* 12 February 2007.
133 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

ALRC's view

4.119 A number of Commonwealth-state cooperative schemes employ a single national regulator to enforce compliance with the scheme. For example, the corporations law scheme is enforced by the Australian Securities and Investments Commission, and the gene technology scheme is enforced by the Gene Technology Regulator.

4.120 The ALRC considers, however, that there are advantages to having a number of agencies and bodies with responsibility for information privacy. These advantages are discussed in Ch 11, and include the pooling of resources, peer review and the promotion of high standards in the performance of regulators, the ability of individuals to approach a local regulator for advice and to make a complaint, and the expertise that an industry-specific dispute resolution body can provide that a general regulator cannot.

4.121 However, the jurisdiction of the various bodies with responsibility for privacy needs to be clarified. Chapter 11 outlines various problems caused by multiple regulators including confusion about where and how to make a privacy complaint, as well as unjustified compliance burden and cost.

4.122 This chapter has outlined a model for national consistency that seeks to clarify the scope of federal, state and territory information privacy laws. It is the ALRC's view that the jurisdiction of the various federal, state and territory bodies with responsibility for information privacy will be clarified once the scope of the *Privacy Act* is clarified in relation to the private sector, and state and territory privacy legislation, amended in accordance with the scheme proposed in this Discussion Paper, is in place.

4.123 There are currently a number of provisions under federal legislation that allow the transfer of complaints concerning information privacy between various bodies.[134] It is the ALRC's view that there are advantages to having privacy complaints dealt with by local regulators. The OPC, however, does not have a power under the *Privacy Act* to delegate its power to state and territory privacy regulators. Therefore, the ALRC has proposed that the *Privacy Act* be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers in relation to complaint handling conferred on the Commissioner by the *Privacy Act*.[135]

4.124 Telstra submitted to the OPC Review that it wanted to see more cooperation between the OPC and other regulators to ensure a national and consistent approach to

---

134 See, eg, *Privacy Act 1988* (Cth) s 50; *Telecommunications Act 1997* (Cth) s 515A; *Ombudsman Act 1974* (NSW) s 6(4A).

135 See Ch 45.

enforcement.[136] One method of achieving this is the development of memoranda of understanding between privacy regulators in relation to enforcement of privacy laws. The ALRC notes that the OPC has already entered into a number of memoranda of understanding with other bodies with responsibility for information privacy, including the Office of the NSW Privacy Commissioner. The ALRC would encourage the OPC to enter memoranda of understanding with each of the bodies with responsibility for information privacy in Australia including industry-specific dispute resolution bodies and state and territory bodies with responsibility for privacy.[137]

4.125 In Chapter 45, the ALRC proposes that the OPC publish documents setting out its complaint-handling policies and enforcement guidelines. These guidelines should address the jurisdiction of the OPC and other bodies involved in the regulation of privacy. For example, the ALRC has proposed that these documents address:

- the roles and functions of the OPC, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Privacy Act*; and

- when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.[138]

4.126 The ALRC has also proposed that the OPC develop and publish educational material in a variety of areas, including material that addresses the various bodies that are able to deal with a complaint in relation to privacy, and when it is appropriate to make a complaint to those bodies.[139] It is the ALRC's view that the OPC's educational material should, where relevant, address the existence of multiple bodies with responsibility for information privacy, and provide guidance on the jurisdiction of each of those bodies.

Other methods to achieve national consistency

4.127 This section of the chapter summarises various methods for dealing with inconsistency and fragmentation in the regulation of personal information that are discussed in detail in other chapters of this Discussion Paper.

---

136 Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

137 The ALRC has proposed the development of memoranda of understanding to clarify the roles of each of the bodies with responsibility for information privacy in the telecommunications industry: see Ch 64.

138 See Ch 64.

139 See Ch 64.

Binding codes

4.128 The OPC Review suggested that one way of overcoming the problems caused by inconsistent state and territory legislation regulating a particular activity is to provide for a power under the *Privacy Act* to develop binding codes.[140] The OPC Review considered that binding codes could be used to regulate a number of areas, at a national level.[141] The OPC reiterated this view in its submission to this Inquiry.[142]

4.129 The Law Council of Australia submitted that a cooperative scheme between the Australian Government and the states and territories utilising the powers to make and impose binding codes of conduct is a possible solution to problems caused by inconsistency and fragmentation. In the Council's view,

> a model along these lines is consistent with the overall 'light touch' approach undertaken in the *Privacy Act*. The introduction of binding codes could clarify the requirements for compliance, and greatly reduce the level of confusion and uncertainty in the current system.[143]

4.130 The OVPC noted that the *Privacy Act* does not authorise the development of joint codes—where codes are developed by more than one regulator. The OVPC submitted that state and territory privacy regulators should be able to review, consult and recommend whether a code be adopted, rather than being required to comply with a code issued by a federal Minister or the federal Privacy Commissioner. This would allow for state and local interests to be reflected better in the final form of code.[144]

4.131 In Chapter 44 of this Discussion Paper, the ALRC proposes a power within the *Privacy Act* for the Privacy Commissioner to develop and impose a privacy code that applies to designated agencies and organisations, or to request the development of a privacy code to be approved by the Privacy Commissioner. This proposal is based on the industry code provisions in Part 6 of the *Telecommunications Act*. It is the ALRC's view that such a power may assist overcoming the problems caused by inconsistent state and territory legislation regulating a particular activity. While the ALRC has not proposed the development of a binding code relating to residential tenancy databases at this stage, it is an example of an area where a binding code could be appropriate in the future.[145]

4.132 A number of state and territory privacy regulators have the ability to make privacy codes.[146] It is the ALRC's view that the proposal to empower the Privacy

---

140 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 7. See discussion of binding codes in Ch 44.
141 Ibid, 159.
142 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
143 Law Council of Australia, *Submission PR 177,* 8 February 2007.
144 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
145 See discussion of residential tenancy databases in Ch 14.
146 See Ch 2.

Commissioner to make or direct the making of a code would not preclude consultation with state and territory privacy regulators when making a code. A memorandum of understanding between the OPC and state and territory privacy regulators could also include a process for consultation with privacy commissioners in other jurisdictions when developing codes.

Non-binding guidelines

4.133 Another option is the making of non-binding guidelines. The Privacy Commissioner publishes a number of non-binding guidelines.[147] This option was considered by the Taskforce on Reducing Regulatory Burdens on Business. Submissions to the Taskforce's review suggested that the OPC could develop voluntary national workplace privacy guidelines. The success of the guidelines would depend on their being widely adopted by business. It was noted that the Privacy Commissioner has already issued guidelines on workplace email, web browsing and privacy. While the guidelines are not legally binding,[148] the Taskforce stated that business has largely adopted them as a benchmark. The Taskforce saw merit in considering this option further in a wider review of the *Privacy Act*.[149]

4.134 The ALRC has made a number of proposals for the OPC and other bodies to develop and publish guidance or non-binding guidelines. For example, the ALRC has proposed that the OPC should provide support to small businesses to assist them in understanding and fulfilling their proposed obligations under the Act, including by developing plain English educational materials—including guidelines—on the requirements under the Act.[150] While non-binding guidelines have the benefit of assisting organisations and agencies to comply with privacy laws, they will not always deal with national consistency issues.

Rules, codes and guidelines

4.135 The potential for inconsistency and complexity to arise because of the development of privacy rules, privacy codes and guidelines by agencies and organisations is discussed in Chapter 11. The ALRC has considered whether the Australian Government should amend the *Privacy Act* to provide that all privacy rules, privacy codes and guidelines developed by agencies and organisations are required to be approved by the Privacy Commissioner. The ALRC did not receive any submissions on this issue. The ALRC considers that such a proposal would have serious resource implications for the OPC, particularly if the ALRC's proposal to remove the small business exemption is implemented. It is the ALRC's view, however, that

147 See, eg, Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998) <www.privacy.gov.au> at 30 July 2007.

148 Office of the Federal Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (2000) <www.privacy.gov.au> at 30 July 2007.

149 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 54.

150 See Ch 35.

organisations and agencies should consult the OPC when developing privacy rules, codes and guidelines.

Guidance on the interaction of legislation

4.136 The complex interactions between the *Privacy Act* and other federal, state and territory regimes that regulate personal information are detailed throughout this Discussion Paper.[151] One issue for consideration is whether the Privacy Commissioner should further develop and publish guidance on the interaction of the *Privacy Act* with other federal, state and territory legislation.[152] Another option for consideration is whether Australian Government and state and territory government agencies that administer legislation that regulates personal information should develop and publish guidance on how that legislation interacts with the *Privacy Act*.

4.137 The OPC Review noted that detailed guidance, issued jointly by the OPC and the body responsible for regulating telecommunications, may assist in increasing understanding of the interaction of the *Privacy Act* and the *Telecommunications Act*. The OPC stated that it would discuss the development of guidance to clarify the relationship between the two Acts.[153] This recommendation has not been implemented to date. The Australian Government Attorney-General's Department has issued guidance on how the *Freedom of Information Act* interacts with the *Privacy Act*.[154]

4.138 In its submission to this Inquiry, the OPC noted that providing greater guidance on the operation of existing laws and how they relate to other regulations will help harmonise current privacy laws.[155] The OVPC submitted that relevant state privacy regulators from the affected jurisdictions should prepare and issue jointly any such guidance.[156]

4.139 The ALRC has made a number of proposals in this Discussion Paper for the OPC to provide guidance on the interaction of legislation, in consultation with other bodies. For example, the ALRC has proposed that the OPC, in consultation with the Australian Communications and Media Authority, Australian Communications Alliance and the Telecommunications Industry Ombudsman, should develop and publish guidelines that outline the interaction between the *Privacy Act*, *Telecommunications Act*, *Spam Act*, and the *Do Not Call Register Act*.[157]

---

151 See, eg, Part H (Health Services and Research) and Part J (Telecommunications).

152 The Privacy Commissioner has power to issue such guidance under *Privacy Act 1988* (Cth) s 27(1)(e).

153 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 10. See also rec 11 relating to the *Spam Act 2003* (Cth).

154 Australian Government Attorney-General's Department, *Freedom of Information Memorandum 93: FOI and the Privacy Act* (1992).

155 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

156 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

157 See Ch 64.

4.140 It is the ALRC's view that, while non-binding guidance does not deal directly with national consistency issues, it does assist individuals, agencies and organisations, and regulators to understand how the *Privacy Act* and other federal, state and territory laws operate and interact. A memorandum of understanding between the OPC and state and territory privacy regulators could include a consultation process when developing guidance on the interaction of federal, state and territory privacy laws.

Scrutiny of legislation

4.141 Section 27 of the *Privacy Act* provides that one of the Privacy Commissioner's functions is to examine (with or without a request from a minister) a proposed enactment that would require or authorise acts or practices that would otherwise be interferences with the privacy of individuals or which may have any adverse effect on the privacy of individuals. Submissions to the OPC Review submitted that this function should be enhanced—for example, the OPC could act as a clearinghouse for ensuring that proposed federal legislation is consistent with the *Privacy Act*.[158] While this function may be used to ensure that federal legislation remains consistent, it may not assist national consistency.[159]

Privacy impact statements and assessments

4.142 Primary legislation and delegated legislation that affect business may require the preparation of a Regulatory Impact Statement (RIS). An RIS is a document prepared by the department, agency, statutory authority or board responsible for a regulatory proposal following consultation with affected parties, formalising some of the steps that must be taken in good policy formulation. It requires an assessment of the costs and benefits of each option, followed by a recommendation supporting the most effective and efficient option. Subject to limited exceptions,[160] the preparation of an RIS is mandatory for all reviews of existing regulation, proposed new or amended regulation and proposed treaties which will directly affect business, have a significant indirect effect on business, or restrict competition.[161]

4.143 One issue is whether a 'privacy impact statement' should accompany any federal, state and territory government proposal to introduce legislation that impinges on privacy.[162] Such a statement could include a privacy impact assessment and an analysis of whether the government proposal is consistent with existing federal, state and territory laws relating to the regulation of privacy. This may include consideration of privacy matters other than the protection of personal information.[163]

---

158 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 44, 46.

159 Ch 44 includes a detailed discussion of this function of the Privacy Commissioner.

160 Australian Government Office of Regulation Review, *A Guide to Regulation—Second Edition: December 1998* (1999), B3–B4.

161 Ibid, B2–B3.

162 N Waters, *Consultation PC 17*, Sydney, 2 May 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

163 Privacy impact assessments are discussed further in Ch 44.

4.144 The NSW Council of Civil Liberties submitted that every parliamentary bill that affects human rights, including privacy, should require a human rights impact assessment.[164] The OVPC noted that federal bills have been enacted without consideration being given to the affect on privacy regulation in Victoria and other jurisdictions. It submitted that a privacy impact assessment should include consideration of whether the proposal is consistent with federal, state and territory privacy laws.[165]

4.145 The ALRC has not proposed that a privacy impact assessment should accompany every federal, state and territory government proposal to introduce legislation that impinges on privacy. It is the ALRC's view that a mandatory requirement of this kind would involve an unjustified compliance burden and cost, and that compliance with a direction to prepare a privacy impact assessment in particular cases can be more effectively monitored than a mandatory requirement. Therefore, the ALRC has proposed that the *Privacy Act* be amended to empower the Privacy Commissioner to direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[166]

4.146 New government projects will often require the enactment of legislation. It is the ALRC's view that when a government agency is conducting a privacy impact assessment of a new project that is supported by legislation, the assessment should address how the new legislation will interact with existing federal, state and territory privacy laws with the aim of maintaining national consistency.

164 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.
165 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
166 See Ch 44.

5. Protection of a Right to Personal Privacy

Contents

Introduction 277
Background 278
Previous ALRC Reports 278
Privacy Act 1988 (Cth) 279
Article 17 of the ICCPR 279
Right to personal privacy—developments in Australia and elsewhere 280
Australia 280
United States 282
Canada 284
New Zealand 285
United Kingdom 286
NSWLRC Consultation Paper on invasion of privacy 290
Recognising an action for breach of privacy in Australia 291
ALRC's view 294
Statutory cause of action 294
Elements of a statutory cause of action 296
Defences 298
Remedies 301
Should the statutory cause of action be in federal legislation? 301
Should the statutory cause of action be in the *Privacy Act*? 303
Limitations on the statutory cause of action 304

Introduction

5.1 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether a cause of action for breach of privacy should be recognised by the courts or the legislature in Australia.[1] It was also noted that, as part of its review of privacy laws in New South Wales, the New South Wales Law Reform Commission (NSWLRC) was looking at the desirability of introducing a statutory tort of privacy in New South Wales.

5.2 The ALRC confirmed that, in an effort to ensure uniform development in this important area of law, the NSWLRC would take primary responsibility for the formulation of proposals for reform. With the consent of those consulted or making a

1 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 1–2.

submission, consultation notes and submissions to the ALRC Inquiry were shared with the NSWLRC.

5.3 In May 2007, the NSWLRC released Consultation Paper 1, *Invasion of Privacy* (NSWLRC CP 1), which is discussed in detail below. The ALRC generally agrees with the proposals for reform put forward in NSWLRC CP 1, therefore the consideration of the issues in this Discussion Paper will be confined to: a brief overview of developments in the law in Australia and elsewhere; a discussion of the submissions and consultations to this Inquiry; and an analysis of NSWLRC CP 1 with particular emphasis on the impact federally of the proposals in that consultation paper. Readers should consider NSWLRC CP 1 when responding to the proposals and question at the end of this chapter.

Background

Previous ALRC Reports

5.4 The ALRC first considered tort protection of privacy in *Unfair Publication: Defamation and Privacy*.[2] After reviewing the existing case law relating to privacy in Australia, proposals by academics and state legislatures aimed at protecting privacy, and approaches to the protection of privacy adopted in overseas jurisdictions, the ALRC proposed a tort of 'unfair publication'. The tort was designed to protect from publication the details of individuals' sensitive private facts relating to their home life, private behaviour, health and personal and family relationships, and to protect against the appropriation for commercial or political purposes of a person's name, identity, reputation or likeness.[3]

5.5 Significantly, the ALRC intended that the scope of the tort would be limited to the publication of 'sensitive' facts. The publication would have to cause distress, embarrassment or annoyance to a person in the position of that individual for an action in tort to lie.[4] For example, the ALRC suggested that the publication, without consent, of a photograph taken in a private place could give rise to an action in the tort of unfair publication where the photograph related to the individual's home life, private behaviour, health, personal and family relationships.[5]

5.6 The ALRC also recommended that an action in tort be available to a person whose name, identity or likeness was published by another person in circumstances where the other person had not obtained the consent of the first person, and published for their own benefit with the intent to exploit the first person's name, identity or

2 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).
3 Ibid, [250].
4 Ibid, [236].
5 Ibid, [240].

likeness. The ALRC confined its recommendation on this issue to matters published for commercial purposes or candidature of office.[6]

5.7 In its later report, *Privacy* (ALRC 22), the ALRC rejected the creation of a general tort of invasion of privacy. In the ALRC's view at that time, 'such a tort would be too vague and nebulous'.[7]

Privacy Act 1988 (Cth)

5.8 During the passage through Parliament of the Privacy Bill 1988 (Cth), the Senate proposed an amendment to the Bill to provide for an action for breach of privacy. The proposed amendment provided that 'interference with the privacy of an individual taking place after the commencement of this Act shall give rise to an action at the suit of the individual for breach of privacy'.[8] The remedies that the Federal Court of Australia or the Supreme Court of a state or territory may award were also stipulated.[9]

5.9 The Senate's proposed amendment was narrower than the general tort of invasion of privacy rejected by the ALRC in ALRC 22. The proposed statutory cause of action would lie only 'against an agency or a tax file number recipient or both'.[10] The House of Representative rejected the proposed amendment.[11]

Article 17 of the ICCPR

5.10 As has been noted in Chapter 1, on 13 August 1980, the Australian Government ratified the *International Covenant on Civil and Political Rights* (ICCPR). Article 17 of the ICCPR states:

> 1. No person shall be subjected to arbitrary or unlawful interferences with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[12]

5.11 In 1988, the Office of the United Nations (UN) High Commissioner for Human Rights released General Comment Number 16, which discussed how the UN interprets

---

6 Ibid, [250].
7 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1081].
8 Parliament of Australia—Senate, *Schedule of the Amendments Made by the Senate to Privacy Bill 1988 (1987–88)* (1988), cl 63A.
9 Ibid, cl 63D.
10 Ibid, cl 63B.
11 Parliament of Australia—House or Representatives, *Schedule of the Amendments Made by the Senate to the Privacy Bill 1988 to which the House of Representatives has Disagreed* (1988).
12 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

art 17 and how it should be promoted through domestic law. It is noted in the General Comment that art 17 should protect a nation's citizens against all interferences and attacks on privacy, family, home or correspondence, 'whether they emanate from State authorities or from natural or legal persons'.[13] To this end, all member states are required 'to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right'.[14] Furthermore, 'state parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons'.[15]

Right to personal privacy—developments in Australia and elsewhere

5.12 A tort of invasion of privacy has, since the 1970s, found legislative expression in some jurisdictions in the United States and Canada. While the courts in the United Kingdom do not recognise such a tort, the equitable action for breach of confidence has been used to address the misuse of private information. In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy; however, the door to the development of such a cause of action at common law has been left open by the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ('*Lenah Game Meats*').[16] To date, two lower courts have held that such a cause of action is part of the common law of Australia.[17]

5.13 The developments in Australia and other comparable overseas jurisdictions cast light on the policy choices available for reform in this area. Of particular interest are the statutory expressions of the tort of invasion of privacy in some of the provinces of Canada[18] and in the Privacy Bill currently before the Irish Parliament,[19] and the development in Australia and the United Kingdom of the test to determine what is considered 'private' for the purpose of determining liability for a breach of privacy.

Australia

5.14 At common law, the major obstacle to the recognition in Australia of a right to privacy was, before 2001, the 1937 High Court decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* ('*Victoria Park*').[20] In a subsequent decision, the

---

13 United Nations Office of the High Commissioner for Human Rights, *General Comment No 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art 17): 08/04/88* (1988), [1].

14 Ibid, [1].

15 Ibid, [9].

16 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

17 These cases are discussed below.

18 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).

19 Privacy Bill 2006 (Ireland).

20 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479. See discussion in D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339,

High Court in *Lenah Game Meats* indicated clearly that the decision in *Victoria Park* 'does not stand in the path of the development of … a cause of action [for invasion of privacy]'.[21] The elements of such a cause of action—and whether the cause of action is to be left to the common law tradition of incremental development or provided for in legislation—remain open questions.[22]

5.15 Two Australian cases have expressly recognised a common law right of action for invasion of privacy. In the 2003 Queensland District Court decision in *Grosse v Purvis*, Skoien SDCJ awarded aggravated compensatory damages and exemplary damages to the plaintiff for the defendant's breach of the plaintiff's privacy.[23] After noting that the High Court in *Lenah Game Meats* had removed the barrier the *Victoria Park* case posed to any party attempting to rely on a tort of invasion of privacy, his Honour took what he viewed as 'a logical and desirable step' and recognised 'a civil action for damages based on the actionable right of an individual person to privacy'.[24]

5.16 While emphasising that 'it is not my task nor my intent to state the limits of the cause of action nor any special defences other than is necessary for the purposes of this case', Skoien SDCJ enumerated the essential elements of the cause of action:

> 1 a willed act by the defendant;
>
> 2 which intrudes upon the privacy or seclusion of the plaintiff;
>
> 3 in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities; and
>
> 4 which causes the plaintiff detriment in the form of mental, physiological or emotional harm or distress, or which prevents or hinders the plaintiff from doing an act which he or she is lawfully entitled to do.[25]

5.17 His Honour noted that a defence of public interest should be available, but that no such defence had been made out on the facts of the case.[26]

341; Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [223].

21 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [107] (per Gummow and Hayne JJ, with whom Gaudron J agreed). See also Ibid, [187] (per Kirby J); [313]–[320] (per Callinan J). For a detailed analysis of the case, see G Taylor and D Wright, 'Australian Broadcasting Corporation v Lenah Game Meats: Privacy, Injunctions and Possums: An Analysis of the Court's Decision' (2002) 26 *Melbourne University Law Review* 707.

22 G Taylor and D Wright, 'Australian Broadcasting Corporation v Lenah Game Meats: Privacy, Injunctions and Possums: An Analysis of the Court's Decision' (2002) 26 *Melbourne University Law Review* 707, 709.

23 *Grosse v Purvis* (2003) Aust Torts Reports 81–706.

24 Ibid, [442].

25 Ibid, [444].

26 Ibid, [34].

5.18 In *Doe v Australian Broadcasting Corporation*, currently the subject of an appeal, the defendant broadcaster published in its afternoon and evening radio news bulletins information that identified the plaintiff—a victim of a sexual assault.[27] In doing so, the defendant breached s 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic), which makes it an offence in certain circumstances to publish information identifying the victim of a sexual offence. Judge Hampel in the County Court of Victoria held that, in addition to breaching a statutory duty owed to the plaintiff by virtue of the *Judicial Proceedings Reports Act,* the defendant broadcaster and two of its employees were liable to the plaintiff in equity for breach of confidence, and in tort for invasion of privacy.[28]

5.19 In holding that a tort for invasion of privacy had been proved, Judge Hampel noted that

> this is an appropriate case to respond, although cautiously, to the invitation held out by the High Court in *Lenah Game Meats* and to hold that the invasion, or breach of privacy alleged here is an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort.[29]

5.20 Responding to the repeated suggestion by defence counsel that recognition of a tort of invasion of privacy would be a 'bold step',[30] her Honour stated:

> If the mere fact that a court has not yet applied the developing jurisprudence to the facts of a particular case operates as a bar to its recognition, the capacity of the common law to develop new causes of action, or to adapt existing ones to contemporary values or circumstances is stultified. Lenah Game Meats, and the UK cases … in particular those decided since Lenah Game Meats, demonstrate a rapidly growing trend towards recognition of privacy as a right in itself deserving of protection.[31]

United States

5.21 In the United States, the *Restatement of the Law, 2nd, Torts* provides for privacy tort protection where:

> 1 One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person;

---

27 *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

28 In *Giller v Procopets* [2004] VSC 113, an earlier case from the Victorian Supreme Court, Gillard J concluded that 'the law has not developed to the point where the law in Australia recognises an action for breach of privacy': *Giller v Procopets* [2004] VSC 113, [188]. See also *Kalaba v Commonwealth* [2004] FCA 763; leave to appeal refused: *Kalaba v Commonwealth* [2004] FCAFC 326. For a critique of *Giller*, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 361–363.

29 *Doe v Australian Broadcasting Corporation* [2007] VCC 281 [157].

30 Ibid, [157].

31 Ibid, [161].

> 2 One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy;
>
> 3 One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public;
>
> 4 One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[32]

5.22 The defences to the privacy torts are subject to the same defences that apply in the United States to defamation.[33] Such defences include an absolute parliamentary and court privilege, consent, and conditional privileges for other activities, such as reporting public proceedings and reasonable investigation of a claim against a defendant.[34]

5.23 The privacy torts have proved to be of limited effect, due in no small part to the existence of a constitutionally entrenched right to a free press. If the subject is newsworthy, and the newsworthy event occurs in a public place, privacy protection tends to take a backseat to the First Amendment protection of freedom of the press.[35] The concept of 'newsworthy' in the United States appears to be broader than the concept of 'public interest', discussed below, applied by the United Kingdom courts in privacy cases.

5.24 California has attempted to provide some additional protection, in particular for celebrities, through the enactment of a cause of action for physical invasion of privacy. This applies

> when the defendant knowingly enters on to the land of another without permission or otherwise commits a trespass in order to physically invade the privacy of the plaintiff with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity and the physical invasion occurs in a manner that is offensive to a reasonable person.[36]

---

32 *Restatement of the Law, 2nd, Torts 1977* (US) §§ 652B, 652C, 652D, 652E.
33 Ibid, §§ 652F–652H.
34 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 343.
35 S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349.
36 *California Civil Code* § 1708.8(a).

5.25 To address the problems associated with an evolving technological environment, § 1708.8 of the *California Civil Code* also establishes an action for constructive invasion of privacy when

> the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or other familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.[37]

5.26 The legislation has been in force since 1998,[38] and the provision's teeth are found in the penalties that apply for committing the invasion, constructive invasion or assault. The penalties include up to three times the amount of general and special damages proximately caused by the invasion, constructive invasion or assault; punitive damages; and possible forfeiture of any proceeds or consideration obtained.[39] Those that direct, solicit, actually induce or cause another person to commit such an assault may also be liable.[40] Whether the legislation survives a constitutional challenge remains to be seen.[41]

Canada

5.27 An individual's right to privacy has received statutory protection in four provinces in Canada.[42] Generally, the legislation provides that 'it is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person'.[43] The legislation also generally stipulates a number of defences, including consent, exercise of a lawful right of defence of person or property, acts or conduct authorised or required by law, privilege and fair comment on a matter

---

37 Ibid § 1708.8(b).

38 The current § 1708.8(c) was enacted in 2005: S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349, 1353.

39 *California Civil Code* § 1708.8(d). If an assault is committed with the intent to capture the visual image, sound recording, or other physical impression of the plaintiff, the penalties in § 17808.8(d)–(h) also apply: *California Civil Code* § 1708.8(c).

40 *California Civil Code* § 1708.8(e).

41 S Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349, 1353–1355.

42 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).

43 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 2. See also *Privacy Act 1996* RSBC c 373 (British Columbia) s 1(1); *Privacy Act* CCSM s P125 (Manitoba) s 2(1); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 3(1). The British Columbia legislation differs from the statutes in force in the other provinces in that it also protects the unauthorised use of the name or portrait of another: *Privacy Act 1996* RSBC c 373 (British Columbia) s 3.

of public interest.[44] Remedies generally include damages, an injunction, an account for profits and an order for the delivery up of material.[45]

5.28 While the *Canadian Charter of Rights and Freedoms 1982*[46] does not guarantee specifically a right to privacy, the Supreme Court of Canada has interpreted the right in s 8 to be secure against unreasonable search and seizure to include a reasonable expectation of privacy in relation to governmental acts.[47] The province of Quebec has guaranteed 'a right to respect for his personal life' in the Quebec *Charter of Human Rights and Freedoms*.[48]

New Zealand

5.29 In *Hosking v Runting*, a majority of the New Zealand Court of Appeal held that the tort of invasion of privacy should be recognised as part of the common law of New Zealand.[49] While the majority stressed that 'the cause of action will evolve through future decisions as courts assess the nature and impact of particular circumstances',[50] the Court was prepared to extend tort protection to wrongful publicity given to private lives. In so holding, the Court of Appeal was influenced by the third formulation of the United States privacy tort[51] when it held that:

> there are two fundamental requirements for a successful claim for interference with privacy:
>
> 1 The existence of facts in respect of which there is a reasonable expectation of privacy; and
>
> 2 Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.[52]

---

44 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 4; *Privacy Act 1996* RSBC c 373 (British Columbia) s 2(2), (3) and (4); *Privacy Act* CCSM s P125 (Manitoba) s 5; *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 5.

45 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 7; *Privacy Act* CCSM s P125 (Manitoba) s 4(1); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 6(1). For an analysis of the impact of the legislation, see S Chester, J Murphy and E Robb, 'Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?' (2003) 27 *Advocates Quarterly* 357.

46 Enacted as Schedule B to the *Canada Act 1982* c 11 (UK), which came into force on 17 April 1982.

47 *R v Dyment* [1988] 2 SCR 417, 426. See also *Godbout v Longueuil (City)* [1997] 3 SCR 844, 913 (s 8 of the *Canadian Charter of Rights and Freedoms* guarantees a sphere of individual autonomy for all decisions relating to 'choices that are of a fundamentally private or inherently personal nature').

48 *Charter of Human Rights and Freedoms* RSQ c–12 (Quebec) s 5. Generally, see the discussion of privacy law in Canada in *Hosking v Runting* [2005] 1 NZLR 1, [60]–[65].

49 For a detailed discussion of *Hosking v Runting* [2005] 1 NZLR 1, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 352–357.

50 *Hosking v Runting* [2005] 1 NZLR 1, [118].

51 Ibid, [118]. The third formulation is outlined above.

52 Ibid, [117].

United Kingdom

5.30 In the United Kingdom, the courts have repeatedly stated that 'English law knows no common law tort of invasion of privacy'.[53] Instead, the cause of action for breach of confidence has been extended to encompass misuse or wrongful dissemination of private information.[54] Extensive expansion of the law in this area has occurred in recent years.

5.31 Professor Des Butler notes that:

> Breach of confidentiality in the United Kingdom has … migrated away from an obligation of confidence to being a doctrine based on the surreptitious means of acquiring private information, thus extending to situations where either: 1 disclosure would be likely to lead to serious physical injury or death of the claimant, and seeking relief from the court is the only way of protecting the claimant; or 2 one person knows or ought to know that another person reasonably expects his or her privacy to be respected.[55]

5.32 In extending the scope of the breach of confidence tort, the courts in the United Kingdom have 'drawn upon the tort of wrongful publication of private facts as developed in the United States of America'.[56]

5.33 In *Ash v McKennitt*, the Court of Appeal recognised that a

> feeling of discomfort arises from the action for breach of *confidence* being employed where there was no pre-existing relationship of confidence between the parties, but the 'confidence' arose from the defendant having acquired by unlawful or surreptitious means information that he should have known he was not free to use …[57]

The court went on to note that, 'at least the verbal difficulty … has been avoided by the rechristening of the tort as misuse of private information: per Lord Nicholls of Birkenhead in *Campbell*'.[58]

5.34 However christened, the developments in the United Kingdom of an action for breach of privacy must now be discussed with reference to the human rights legislation in force in the European Union. The European Convention on Human Rights came into force in the United Kingdom in October 2000.[59] Since that time, the courts in the

---

53 *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920, [272]. See also *Wainwright v Home Office* [2004] 2 AC 406.

54 B McDonald, 'Privacy, Princesses, and Paparazzi' (2005–2006) 50 *New York Law School Law Review* 205, 232. See also *Hosking v Runting* [2005] 1 NZLR 1, [23]–[53].

55 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 350.

56 *Hosking v Runting* [2005] 1 NZLR 1, [43].

57 *Ash v McKennitt* [2007] 3 WLR 194, [8] (emphasis in text).

58 Ibid, [8].

59 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 10 December 1948, Council of Europe, ETS No 005, (entered into force generally on 3 September 1953). The Convention was implemented by the *Human Rights Act 1998* (UK).

United Kingdom have been influenced by art 8 of the Convention,[60] and by the Strasbourg jurisprudence interpreting art 8.[61]

5.35 When analysing whether the elements of the tort have been established in a case of unlawful publication of private information (which constitutes the majority of the case law in the United Kingdom), the court engages in a two-part balancing exercise. The court first ascertains whether the information is private 'in the sense that it is in principle protected by article 8'.[62] If the answer is 'yes', the court then asks: 'in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by article 10'? [63]

5.36 The courts in the United Kingdom have avoided setting too high a bar when determining what 'private' means within the context of art 8. When considering the first limb of the test, the person alleging a breach of art 8 must establish that interference with private life was of 'some seriousness' before art 8 is engaged.[64]

5.37 It is unclear whether 'some seriousness' equates to, or is less than, the standard of disclosure that is 'highly offensive to a reasonable person of ordinary sensibilities', propounded in cases such as *Lenah Game Meats*. In *Campbell v MGN Ltd*, Nicholls LJ warned that the 'highly offensive' formulation

> should be used with care for two reasons. First, the 'highly offensive' phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the 'highly offensive' formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion. [65]

5.38 Hope LJ noted that the threshold test is 'what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity'.[66] Baroness Hale LJ suggested a similar formulation.[67]

5.39 Once the information is identified as 'private', the court must then 'balance the claimant's interest in keeping the information private against the countervailing interest of the recipient in publishing it'.[68] This balancing test is contextual—that is,

---

60 Article 8(1) provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'.
61 *Ash v McKennitt* [2007] 3 WLR 194, [11].
62 Ibid, [11].
63 Ibid, [11].
64 Ibid, [12]; *M v Secretary of State for Work and Pensions* [2006] 2 AC 91, [83].
65 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
66 Ibid, [99].
67 Ibid, [136].
68 Ibid, [137].

determined by reference to the facts of the particular case. The principles formulated by the trial judge in *McKennitt v Ash*, and endorsed by the Court of Appeal, to determine the second limb of the test are:

> i) Neither article [8 and 10 of the European Convention on Human Rights] has as such precedence over the other.
>
> ii) Where conflict arises between the values under Articles 8 and 10, an 'intense focus' is necessary upon the comparative importance of the specific rights being claimed in the individual case.
>
> iii) The court must take into account the justifications for interfering with or restricting each right.
>
> iv) So too, the proportionality test must be applied to each.[69]

5.40 In *Von Hannover v Germany*,[70] a decision of the European Court of Human Rights which has been followed in the United Kingdom,[71] the Court established the benchmark from which an analysis of the application of art 8 must proceed. First, the Court recognised the 'fundamental importance of protecting private life from the point of view of the development of every human being's personality'.[72] The Court noted that the protection 'extends beyond the private family circle and also includes a social dimension … anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection of and respect for their private life'.[73]

5.41 It is clear from the reasoning in *Von Hannover v Germany* that the court took into account, to use the words found in the Terms of Reference for this Inquiry,[74] 'the need of individuals for privacy in an evolving technological environment'. The Court stressed the fact that 'increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data'.[75]

5.42 The Court also acknowledged the essential role played by the press in a democratic society, and in particular in the exercise of the right of freedom of expression.[76] This role, however, is circumscribed if, for example, the publication interferes with the privacy of an individual. If freedom of expression is to take precedence over an individual's right to privacy, the interference must be in the public interest. In this context, 'what interests the public is not necessarily in the public interest'.[77]

---

69 *Ash v McKennitt* [2007] 3 WLR 194, [46].
70 *Von Hannover v Germany* [2004] ECHR 294.
71 See, eg, *Ash v McKennitt* [2007] 3 WLR 194, [58]–[59].
72 *Von Hannover v Germany* [2004] ECHR 294, [69].
73 Ibid, [69].
74 The Terms of Reference are reproduced at the beginning of this Discussion Paper.
75 *Von Hannover v Germany* [2004] ECHR 294, [70].
76 Ibid, [58].
77 *Ash v McKennitt* [2007] 3 WLR 194, [66].

5.43 In *Jameel v Wall Street Journal Europe*, Baroness Hale LJ, in commenting on 'the obligation of the press, media and other publishers to communicate important information upon matters of general public interest and the general right of the public to receive such information',[78] noted:

> The public only have a right to be told if two conditions are fulfilled. First, there must be a real public interest in communicating and receiving the information. This is, as we all know, very different from saying that it is information which interests the public—the most vapid tittle-tattle about the activities of footballers' wives and girlfriends interests large sections of the public but no-one could claim any real public interest in our being told all about it … Secondly, the publisher must have taken care that a responsible publisher would take to verify the information published.[79]

5.44 The first condition has also been held to apply to a determination involving a conflict between art 8 and art 10 rights.[80]

5.45 In a recent case, JK Rowling, the author of the phenomenally successful *Harry Potter* series, and her husband sued a photo agency on behalf of their 18 month old son. The agency's photographer took a covert photograph of the couple and their son on a street in Edinburgh. The photograph, which was published in a newspaper, clearly showed the son's profile. Rowling and her husband claimed that the photograph breached their son's right to privacy, and that its publication was a misuse of private information.[81]

5.46 In dismissing the case before trial, Patten J stated:

> If a simple walk down the street qualifies for protection then it is difficult to see what would not. For most people who are not public figures in the sense of being politicians or the like, there will be virtually no aspect of their life which cannot be characterized as private. Similarly, even celebrities would be able to confine unauthorized photography to the occasions on which they were at a concert, film premiere or some similar function.[82]

5.47 Patten J went on to note that 'even after *Von-Hannover* there remains, I believe, an area of routine activity which when conducted in a public place carries no guarantee of privacy'.[83] If the decision is not overturned on appeal, it has the potential to limit the breadth of *Von Hannover v Germany*.[84]

---

78 *Jameel v Wall Street Journal Europe* [2006] 2 AC 465, [146]. In the United Kingdom this is known as the 'Reynolds privilege' or 'Reynolds defence' after the decision in *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127.

79 *Jameel v Wall Street Journal Europe* [2006] 2 AC 465, [147].

80 *Ash v McKennitt* [2007] 3 WLR 194, [66].

81 *Murray v Express Newspapers PLC* [2007] EWHC 1908.

82 Ibid, [65].

83 Ibid, [66].

84 *Von Hannover v Germany* [2004] ECHR 294.

NSWLRC Consultation Paper on invasion of privacy

5.48 As has been noted above, the NSWLRC has, as part of its review of privacy law in New South Wales, released a Consultation Paper that discusses whether a statutory cause of action for invasion of privacy should be introduced in that state. The NSWLRC has reached the preliminary view that persons should be protected in a broad range of contexts from unwanted intrusions into their private lives or affairs.[85] A statutory model to ensure such protection is put forward for consultation.[86] A case for reform is articulated in Chapter 1 of NSWLRC CP 1 and will not be repeated here.

5.49 After an extensive review of developments in Australia and overseas, the NSWLRC considered four possible statutory models:

> 1. One general, non-specific right to seek redress for invasion of personal privacy.
>
> 2. A general cause of action for invasion of privacy, supplemented by a non-exhaustive list of the circumstances that could give rise to the cause of action.
>
> 3. A general cause of action for invasion of privacy, together with other specific statutory causes of action, for example, in respect of unauthorised surveillance activity.
>
> 4. Several narrower and separate causes of action based on various distinct heads of privacy.[87]

5.50 The second option, which is the one favoured by the NSWLRC, is modelled on the existing law in the Canadian provinces of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador.[88] It is also the model upon which the Privacy Bill currently before the Irish Parliament is based.[89] Unlike the Canadian and Irish statutes, which frame the cause of action in tort, the NSWLRC suggests that the cause of action should be expressed in terms of a right of action for invasion of privacy, rather than as a tort of violation of privacy.

5.51 The NSWLRC suggests the following as an example of a statutory cause of action:

> A person would be liable under the Act for invading the privacy of another, if he or she:
>
> (a) interferes with that person's home or family life;
>
> (b) subjects that person to unauthorised surveillance;
>
> (c) interferes with, misuses or discloses that person's correspondence or private written, oral or electronic communication;

---

85 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [1.20].
86 Ibid, proposal 1.
87 Ibid, [6.2].
88 *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act 1978* RSS c P–24 (Saskatchewan); *Privacy Act* CCSM s P125 (Manitoba); *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador).
89 Privacy Bill 2006 (Ireland).

(d) unlawfully attacks that person's honour and reputation;

(e) places that individual in a false light;

(f) discloses irrelevant embarrassing facts relating to that person's private life;

(g) uses that person's name, identity, likeness or voice without authority or consent.

This list should be interpreted as illustrative and not exhaustive.[90]

5.52 Having suggested that a general cause of action for invasion of privacy could be provided for by statute, the NSWLRC goes on to discuss the essential elements of the cause of action. The defences to such a cause of action are also discussed. On these issues, the NSWLRC calls for submissions and refrains from making any proposals.[91]

5.53 In the final chapter, the NSWLRC explores a range of common law, equitable and statutory remedies that could be available to a person who has had his or her privacy unlawfully invaded. The Commission proposes that:

> The statute should provide that where the court finds that there has been an invasion of the plaintiff's privacy, the Court may, in its discretion, grant any one or more of the following:
>
> - damages, including aggravated damages, but not exemplary damages;
> - an account of profits;
> - an injunction;
> - an order requiring the defendant to apologise to the plaintiff;
> - a correction order;
> - an order for the delivery up and destruction of material;
> - a declaration;
> - other remedies or orders that the Court thinks appropriate in the circumstances.[92]

5.54 The NSWLRC is currently conducting consultations on its proposals. The ALRC understands that the NSWLRC intends to have its final report completed in early 2008.

Recognising an action for breach of privacy in Australia

5.55 In IP 31, the ALRC asked the following question:

---

90 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [6.32].
91 Ibid, [7.60].
92 Ibid, Proposal 2.

> Should a cause of action for breach of privacy be recognised by the courts or the legislature in Australia? If so, and if legislation is preferred, what should be the recognised elements of the cause of action, and the defences? Where should the cause of action be located? For example, should the cause of action be located in state and territory legislation or federal legislation? If it should be located in federal legislation, should it be in the *Privacy Act* or elsewhere?[93]

5.56 There was general support for the recognition of a cause of action for breach of privacy in the submissions that addressed the question.[94] A significant minority, however, expressed serious reservations.[95] Comment on the question was more widespread in consultations, and the support for and against was similar to that evidenced in submissions.

5.57 The comments in the submission of the Centre for Law and Genetics are representative of the types of comments expressed by those who favoured the enactment of a statutory cause of action.

> It is most surprising that the Australian courts have yet to develop common law or equitable principles for breach of privacy in Australia. Australia is becoming increasingly out of step with other common law jurisdictions in this regard. It may well be that the courts would be amenable to such a development, should the right case come before them. In the absence of common law or equitable protection, there is good justification for the development of legislation to fill the void.[96]

5.58 In support of its view that a cause of action for breach of privacy should be recognised, AAMI noted:

> International law is moving this way, thus it would be logical to include this concept. Social expectations are also moving in this direction, especially with the advent of the internet and digital technology. Preferred method is statutory, as it's a lot easier for businesses to digest and apply.[97]

5.59 Of those expressing support for a cause of action, statutory enactment in federal legislation was the preferred option. The Office of the Privacy Commissioner (OPC) suggested that, when formulating the elements of a statutory cause of action, the focus

---

93 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 1–2.

94 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; J Carland and J Pagan, *Submission PR 42,* 11 July 2006; M Lyons and B Le Plastrier, *Submission PR 41,* 11 July 2006.

95 Telstra, *Submission PR 185,* 9 February 2007; Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

96 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

97 AAMI, *Submission PR 147,* 29 January 2007.

should be on torts relating to invasion of privacy, and in particular unreasonable intrusion upon privacy and disclosure of private facts.[98]

5.60 The OPC noted that, while the nature of any defences would depend on the specific wording of the torts, the most significant likely defences would be: express or implied consent; public interest, and in particular, this defence should cover 'the existing freedom of communication concerning government or political matters … as well as matters of public concern'; and other defences based on existing defences in defamation.[99]

5.61 The arguments raised by stakeholders against the enactment of a cause of action fall into the following categories:

- the privacy of Australians is adequately protected under the current regulatory regime;[100]
- recognition of a cause of action for breach of privacy is best left to incremental development at common law through the courts;[101] and
- a statutory cause of action for breach of privacy will tip the balance too heavily in favour of privacy rights for individuals at the expense of the free flow of information on matters of public concern,[102] and the benefits to society flowing from artists who create art in public places, for example photographers.[103]

5.62 Media organisations, in particular, were concerned that a statutory cause of action for breach of privacy would 'be just another weapon in the arsenal of those in society who would seek to deflect public scrutiny of their possible malfeasance or non-feasance'.[104] The Australian Press Council stated:

> In the development of any proposal towards a putative cause of action for breach of privacy, the Commission needs to place a stress on the public interest as an appropriate criterion to be used to determine the balance between privacy rights for

98 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007. The OPC suggested that the elements of a tort of privacy proposed by Professor Butler, in D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, would be a useful model for the ALRC to consider.

99 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

100 Telstra, *Submission PR 185,* 9 February 2007; AXA, *Submission PR 119,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

101 Telstra, *Submission PR 185,* 9 February 2007.

102 SBS, *Submission PR 112,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

103 Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007.

104 Australian Press Council, *Submission PR 48,* 8 August 2006.

> individuals and the public's right to the free flow of information on matters of public concern.[105]

5.63 SBS stressed that, 'being able to film or gather information without restrictions is important not only for the proper reporting of news and current affairs items, but also, for example, in projects which reflect Australian society'.[106] The Arts Law Centre of Australia expressed a related concern that 'a cause of action for breach of privacy would limit the creativity and expression of the Australian artists whose work takes on a documentary focus and attempts to capture everyday life, people and public space'.[107]

ALRC's view

Statutory cause of action

5.64 In the absence of a statutory cause of action, the common law in this area will continue to develop. Whether this evolution results in the recognition of a tort of invasion of privacy, the adoption by Australian courts of the United Kingdom's approach to breach of confidence, a combination of the two or a rejection of the international trend, is a question for the courts.

5.65 If Australian courts follow the United Kingdom's approach of developing the cause of action within the equitable action for breach of confidence, or decide tort law should be the preferred vehicle, they will have to develop the cause or causes of action within the rules of equity and tort. This has an impact on the circumstances that will be recognised as giving rise to the cause of action, and on the remedies available to address the wrong.

5.66 Sir Roger Toulson, co-author of a leading text on confidentiality[108] and a judge of the England and Wales Court of Appeal, has highlighted, in the context of the United Kingdom's approach, a limitation inherent in the incremental development of the common law. He identifies an important limitation on the use of breach of confidence to address privacy issues.

> A consequence of the development of privacy within the action for breach of confidentiality is that it is presently confined to cases involving the use of information of a private nature, whether in word or pictorial form. So however strong and understandable may be the feeling of harassment of a person who is hounded by photographers when carrying out activities of a private nature, and however unacceptable the behaviour of the pack, there will be no cause of action until an intrusive photograph is published. From the viewpoint of the mischief against which Article 8 [of the *Human Rights Act* (1998)] is aimed, this is illogical.[109]

---

105 Ibid.
106 SBS, *Submission PR 112,* 15 January 2007.
107 Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007.
108 R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006).
109 R Toulson, 'Freedom of Expression and Privacy' (Paper presented at Association of Law Teachers Lord Upjohn Lecture, London, 9 February 2007), 7.

5.67 To put these comments in an Australian context, if the United Kingdom's approach applied, the plaintiff in *Doe v ABC* would (and did on the findings of the trial judge) have a recognised cause of action for breach of confidence, but the plaintiff in *Grosse v Purvis* would be without a remedy.

5.68 Such constraints can be overcome if a statutory cause of action for invasion of privacy is enacted. This avoids the problems inherent in attempting to fit all the circumstances that may give rise to an invasion of privacy into a pre-existing cause of action—such as breach of confidence—or formulating a previously unrecognised cause of action—such as the tort of invasion of privacy. It also allows for a more flexible approach to defences and remedies.[110]

5.69 The ALRC agrees with the preliminary view of the NSWLRC that individuals should be protected from unwanted intrusions into their private lives or affairs in a broad range of contexts, and proposes that a statutory cause of action is the best way to ensure such protection. It forecloses the possibility of Australia adopting breach of confidence as the primary vehicle to protect from invasion an individual's private life, and alleviates the necessity of judges taking the 'bold step'[111] of formulating a new tort. Further, it does away with the distinction between equitable and tortious causes of action, and between the defences and remedies available under each. Finally, and importantly, this view is supported by a majority of those making submissions to the Inquiry on this issue, and by a majority of those consulted to date.

5.70 It follows that the ALRC supports the NSWLRC's preliminary view that the 'statutory cause of action for invasion of privacy should not be constrained at the outset by an assumption that rules otherwise applicable to torts generally should necessarily apply to the statutory cause of action for invasion of privacy'.[112] In addition, as the NSWLRC notes, this approach allows for the consideration of competing interests, including the public interest, 'that have not traditionally been relevant in the development of tortious causes of action'.[113]

5.71 The ALRC's view is that it is also appropriate to set out a non-exhaustive list of the types of acts or conduct that could constitute an invasion of privacy. Whether all of the categories set out in the example put forward in NSWLRC CP 1 should be adopted is a separate issue.[114]

---

110 A case note on *Doe v ABC* published in the *Australian Press Council News* noted, 'if a privacy tort were defined by statute, it could incorporate workable defences. In addition to a strong public interest defence, a defence could be based on an appropriate offer-of-amends procedure': I Ryan, 'Doe v ABC—A Case Note' (2007) 19(2) *Australian Press Council News* <www.presscouncil.org.au>, 7.

111 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, [157].

112 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [1.7].

113 Ibid, [1.7].

114 Ibid, [6.32].

5.72 In particular, it is questionable whether an unlawful attack on a person's honour and reputation, placing a person in a false light and using a person's name, identity, likeness or voice without authority or consent are properly characterised as invasions of privacy. It has been argued, at least in relation to false light and appropriation, that such conduct is better left to the law of defamation.[115] The same argument applies to an unlawful attack on a person's honour and reputation, which clearly falls within the parameters of defamation law.[116]

5.73 In *Lenah Game Meats,* Gummow and Hayne JJ commented on the tenuous nexus between privacy and the appropriation and false light torts.

> Whilst objection possibly may be taken on non-commercial grounds to the appropriation of the plaintiff's name or likeness, the plaintiff's complaint is likely to be that the defendant has taken the steps complained of for a commercial gain, thereby depriving the plaintiff of the opportunity of commercial exploitation of that name or likeness for the benefit of the plaintiff. To place the plaintiff in a false light may be objectionable because it lowers the reputation of the plaintiff or causes financial loss or both. The remaining categories [of the *Restatement of the Law, 2nd, Torts, 1977* (US)], the disclosure of private facts and unreasonable intrusion upon seclusion, perhaps come closest to reflecting a concern for privacy 'as a legal principle drawn from the fundamental value of personal autonomy', the words of Sedley LJ in *Douglas v Hello! Ltd*.[117]

5.74 It has also been suggested that the appropriation tort is a form of intellectual property, in that it protects a property right as distinct from the privacy of a person. Alternatively, an extension of the tort of 'passing off', or the development of a 'right of publicity', may be a better way to deal with the perceived problem.[118]

Elements of a statutory cause of action

5.75 The NSWLRC suggests two possible approaches to establishing the elements of a statutory cause of action for invasion of privacy.

> An invasion of privacy could be determined as made out where:
>
> - The plaintiff had, in all the circumstances, a reasonable expectation of privacy in relation to the relevant conduct or information; and/or

115 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 368.

116 See, eg, s 3(c) of the uniform *Defamation Act 2005* in force in NSW, Vic, Qld, SA, Tas, WA and NT.

117 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [125].

118 For a discussion of the application to appropriation cases of intellectual property law, the tort of 'passing off' and the development of a 'right of publicity', see R Zapparoni, 'Propertising Identity: Understanding the United States Right of Publicity and it's Implications—Some Lessons for Australia' (2004) 28 *Melbourne University Law Review* 690. For a discussion of information privacy as a form of property, see J Rule, 'Towards Strong Privacy: Values, Markets, Mechanisms, and Institutions' (2004) 54 *University of Toronto Law Journal* 183. A contrary view is discussed in R Toulson and C Phipps, *Confidentiality* (2nd ed, 2006), [2–056]–[2–066].

- The defendant's invasion of that privacy in relation to that conduct or information, is, in all the circumstances, offensive (or highly offensive) to a reasonable person of ordinary sensibilities.[119]

5.76 The fact that the two approaches are not mutually exclusive is evidenced by *Hosking v Runting*. As has been noted above, the court found that the fundamental requirements for a successful interference with privacy, in the context of wrongful publicity given to private lives, includes both a reasonable expectation of privacy and conduct that would be considered highly offensive to the hypothetical reasonable person.[120]

5.77 The NSWLRC concedes that these two approaches 'may often be two sides of the same coin. They are not necessarily mutually exclusive'. It suggests, however, that this may not always be the case. To illustrate this point, the NSWLRC gives the example of a medical practitioner who reveals the plaintiff's HIV status by mistake. The NSWLRC suggests that the plaintiff may have a reasonable expectation of privacy, but that the disclosure of the plaintiff's HIV status will not be 'highly offensive to a reasonable person of ordinary sensibilities'.[121]

5.78 Such a distinction illustrates the point made by Nicholls LJ in *Campbell v MGN Ltd*, noted above. The 'highly offensive' formulation should be approached with care; one reason being that the phrase 'highly offensive' is suggestive of a stricter test of what should be considered private than a reasonable expectation of privacy.[122]

5.79 The ALRC's view is that, in determining what is considered 'private' for the purpose of establishing liability under the statutory cause of action, there must be *both* a reasonable expectation of privacy in all the circumstances, and the act complained of must satisfy an objective test of seriousness. In determining the latter, the bar should not be set too high.

5.80 Adopting the phrase used by Gleeson CJ in *Lenah Game Meats*—that is, 'highly offensive to a reasonable person of ordinary sensibilities'[123]—may be too high a threshold. A more appropriate test of seriousness may be where the act complained of is, in all the circumstances, sufficiently serious to cause substantial offence to a person of ordinary sensibilities.[124]

---

119 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.5].
120 *Hosking v Runting* [2005] 1 NZLR 1, [117].
121 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.6].
122 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
123 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].
124 See R Toulson, 'Freedom of Expression and Privacy' (Paper presented at Association of Law Teachers Lord Upjohn Lecture, London, 9 February 2007), 7.

The role of consent

5.81 Consent, whether express or implied by the plaintiff or some person entitled to consent on the plaintiff's behalf, will, in most cases, provide an answer to a cause of action for invasion of privacy. Legislatively, it can be dealt with in the following ways.[125] It can:

- be included as an essential element of the cause of action—for example, to use 'letters, diaries or other personal documents of a person … *without the consent, express or implied, of the person or some other person who has the lawful authority to give the consent*', may in a variety of circumstances constitute an invasion of privacy;[126]

- be considered when determining whether there was a reasonable expectation of privacy in all the circumstances, or as a circumstance in determining whether the act complained of meets the test of 'sufficiently serious to cause substantial offence to a person of ordinary sensibilities';

- operate as an exception to the general cause of action;[127] or

- be a defence to an action.[128]

5.82 The ALRC's view is that, when formulating a statutory cause of action for invasion of privacy, issues of consent are best dealt with in the context of an essential element of the cause of action, when determining whether the plaintiff had a reasonable expectation of privacy in the circumstances or when determining whether the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities. This is consistent with the approach to consent adopted in the protection of personal information. Consent is considered when determining whether there has been a breach of the proposed Unified Privacy Principles, not as a defence to justify a breach.[129]

Defences

5.83 The defences to a cause of action for invasion of privacy generally include where the:

---

125 Generally see New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.12]–[7.17].

126 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 3(d) (emphasis added).

127 *Privacy Act 1996* RSBC c 373 (British Columbia) s (2)(a).

128 *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s5(1)(a); *Privacy Act 1978* RSS c P–24 (Saskatchewan) s4(1)(a); *Privacy Act* CCSM s P125 (Manitoba) s5(a). See also, Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy* (2004), recs 4, 9.

129 The role of consent in the context of the proposed Unified Privacy Principles is discussed in detail in Ch 16.

- act or conduct was incidental to the exercise of a lawful right of defence of person or property;
- act or conduct was authorised or required by or under law;
- disclosure of information was of public interest or was fair comment on a matter of public interest; or
- disclosure of information was, under defamation law, privileged.[130]

Public interest

5.84 Of particular concern in the context of this Inquiry is the defence of public interest, or fair comment on a matter of public interest. In this context, the circumstances giving rise to an invasion of privacy may also involve a competing right of freedom of expression.

5.85 The public interest defence commonly arises, as the above review of the case law illustrates, when private information is published. Perhaps less notoriously, it can also arise when artists and documentary filmmakers attempt 'to capture everyday life, people and public space'.[131] When the defence is raised, the court will have to determine if, in all the circumstances, the public interest asserted outweighs the individual's right to privacy.[132]

5.86 Recognition of the public interest defence simply reflects the fact that the right to privacy is not absolute. In appropriate circumstances, it will have to give way to other competing rights, such as freedom of expression. The ALRC agrees with the Australian Press Council that public interest is an essential criterion to be used to determine 'the balance between privacy rights for individuals and the public's right to the free flow of information on matters of public concern'.[133]

5.87 It is important to keep in mind, however, that 'freedom of expression' and 'freedom of the press' are not synonymous, although the latter often facilitates the former. Professor Eric Barendt notes:

> Press freedom is parasitic to some extent on the underlying free speech rights and interests of readers and listeners, and the role which the press and other media play in informing them. It is not the same as the free speech argument, and that should be

---

130 For example see *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 5; Privacy Bill 2006 (Ireland) cl 5(1) and 6. For the types of disclosure covered by privilege in defamation law, see ss 27 and 30 of the Uniform *Defamation Act 2005* in force in NSW, Vic, Qld, SA, Tas, WA and NT.

131 Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007. See also SBS, *Submission PR 112,* 15 January 2007.

132 See *Aubry v Éditions Vice Versa Inc* [1998] 1 SCR 591.

133 Australian Press Council, *Submission PR 48,* 8 August 2006.

> borne in mind when we consider how much weight should be attached to the freedom when it conflicts with the right to privacy which certainly is a fundamental human right.[134]

5.88 While Barendt's comments are couched in the language of 'free speech rights', which is a right expressly recognised in the *United States Constitution*, the underlying rationale applies equally in an Australian context. The result is that publication of personal information may constitute an invasion of privacy if the privacy interest asserted by the plaintiff outweighs any public interest asserted by the defendant.

Authorised or required by or under law

5.89 Another important defence is that the act or conduct was authorised or required by or under law. This defence assumes particular importance in the context of law enforcement and national security.

5.90 In Chapter 13, the scope of this exception in the context of the *Privacy Act* is discussed in detail. Generally, the ALRC's view is that the *Privacy Act* should not fetter a government's discretion to require or authorise that personal information be handled in a particular way. It follows, therefore, that a requirement that the act or conduct was required or authorised by or under law would be a defence to the statutory cause of action.

5.91 The ALRC asks whether the definition of a 'law' for the purpose of determining when an act or practice is required or specifically authorised by or under a law includes:

- a common law or equitable duty;
- an order of a court or tribunal;
- documents that are given the force of law by an Act of Parliament, such as industrial awards; and
- statutory instruments, such as a Local Environmental Plan made under a planning law.[135]

5.92 Stakeholder responses to this question will assist the ALRC to develop a final view on the scope of this defence to the statutory cause of action.

---

134 E Barendt, 'Privacy and Freedom of Speech' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 11, 23.

135 See Question 13–1.

Remedies

5.93 In NSWLRC CP 1, the NSWLRC, as has been noted above, articulates the range of remedies that could be used to address an invasion of privacy. Given the wide range of circumstances in which an action for invasion of privacy may be brought under the statute, the ALRC agrees with the NSWLRC that it makes sense to 'enable the court to choose the remedy that is most appropriate in the fact situation before it, free from the jurisdictional constraints that may apply to that remedy in the general law'.[136] The underlying rationale, and a description of the range of appropriate remedies, is discussed in NSWLRC CP 1.[137]

Should the statutory cause of action be in federal legislation?

5.94 Having proposed statutory recognition of a cause of action for invasion of privacy, a question arises as to where the cause of action should be located. For example, should the cause of action be located in state and territory legislation or federal legislation? If the latter, should it be in the *Privacy Act* or elsewhere?[138]

5.95 Inconsistency and fragmentation of laws regulating the handling of personal information is, as detailed in Part C, a major issue in this Inquiry. To avoid a similar problem arising in relation to the enactment of a statutory cause of action for invasion of privacy, it is desirable to ensure national consistency from the outset. Models for achieving national consistency are canvassed in detail in Chapter 4.

5.96 Supporters of a statutory cause of action also issued a plea for uniformity. The Centre for Law and Genetics, for example, stated that, if a statutory cause of action is developed, 'it is critically important that it should be consistent across Australia, either as uniform state and territory legislation through agreement between the relevant Ministers, or as federal legislation'.[139] The OPC noted that

> it would be preferable to introduce a tort of privacy in a uniform manner throughout Australia, particularly to avoid inconsistencies and 'forum shopping' … Nevertheless, by what method a tort would be established and in what manner it would be introduced, it should not contribute to the national inconsistency that currently exists in the privacy laws arena.[140]

5.97 Most of those in favour of a statutory cause of action expressed the view that it be enacted in federal legislation. The Queensland Government, for example, recommended that, 'if implementation of a statutory cause of action for breach of

---

136 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [8.3].
137 Ibid, Ch 8.
138 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 1–2.
139 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
140 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

privacy is proposed, such a cause of action should be located in federal legislation'.[141] AAMI stated, 'the legislation should definitely be federal (one set of rules for the whole country). The *Privacy Act* is the logical place for it'.[142]

5.98 Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave of the Cyberspace Law and Policy Centre suggested that:

> Given that the Commonwealth has asserted constitutional power in relation to the protection of privacy in the private sector, it may be consistent with this for the Commonwealth to also legislate, in the Privacy Act, for a statutory tort or torts to protect other aspects of privacy in relation to the private sector. It will be necessary to carefully align the elements of a statutory privacy tort with what is already protected by privacy principles.[143]

5.99 For the reasons noted in Chapter 4, the federal government has the constitutional power to enact a statutory cause of action for invasion of privacy, to the exclusion of state and territory legislation. The federal government could decide, however, to include a provision that provides that the federal Act is not intended to exclude or limit the operation of a law of a state or territory that is capable of operating concurrently with the federal Act.[144]

5.100 If this policy option prevails, it is essential to ensure that the states and territories enact uniform legislation. Failure to do so would give rise to the fragmentation and inconsistency that has characterised the regulation of information privacy.

5.101 The ALRC's view is that, to ensure uniformity and to avoid the problems associated with inconsistent legislation, the statutory cause of action for invasion of privacy should be in federal legislation and should cover federal agencies, organisations and individuals. It should also cover state and territory public sector agencies until such time as uniform state and territory legislation is enacted.[145]

5.102 The ALRC acknowledges that this approach differs from the proposed model for reform of information privacy legislation relating to the state and territory public sectors discussed in Chapter 4. The difference is warranted, however, because the handling of personal information is currently regulated in all state and territory public sectors. As no states or territories currently have a statutory cause of action for invasion of privacy, failure to extend the coverage of the cause of action to state and territory public sectors would result in gaps in coverage, rather than simply inconsistent regulation.

---

141 Queensland Government, *Submission PR 242,* 15 March 2007.
142 AAMI, *Submission PR 147,* 29 January 2007.
143 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
144 For an example of such a provision, see the *Age Discrimination Act 2004* (Cth) s 12(3).
145 The distinction between federal, state and territory agencies is discussed in detail in Ch 34.

Should the statutory cause of action be in the *Privacy Act*?

5.103 The prevailing view of supporters of a cause of action for invasion of privacy is that the cause of action be enacted in federal legislation. The OPC suggests that the role, if any, to be played by the Privacy Commissioner should determine the location of the cause of action.

> If the tort is actionable via the complaints process administered by the Privacy Commissioner, then there may be merit in streamlining all privacy-related complaints through this process. By contrast, if the tort will be actionable directly in the Courts it may be preferable to create a separate statute, to distinguish the tort of invasion of privacy from complaints handled under the Privacy Act.[146]

5.104 The proposed cause of action for invasion of privacy is broader than simply information privacy—the current focus of the *Privacy Act*. Disclosure of personal information may give rise, however, to both a breach of the privacy principles and liability under the cause of action. Conversely, adherence to guidelines issued by the OPC, or protocols designed to ensure compliance with privacy principles, may be a relevant factor in determining whether the privacy principles have been breached, or the elements of the cause of action made out.

5.105 The same circumstances, therefore, may give rise to a complaint to the Privacy Commissioner under the *Privacy Act*, and an action in court for invasion of privacy. While the statute could provide that an individual must choose either to lodge a complaint or institute a cause of action, the ALRC's view is that such a requirement is undesirable. An individual should be able to choose the forum that will provide the most appropriate remedy. The costs associated with pursuing the action or complaint will also be a relevant factor. Further, if pursuing both avenues simultaneously can be shown to be unfair, the proceedings in one forum may be stayed pending the outcome in the other forum.[147]

5.106 Finally, the Privacy Commissioner should play a role in educating the public about the existence of the statutory cause of action.

5.107 In summary, the ALRC's view is that the *Privacy Act* should be amended to include a new part setting out the provisions relating to the cause of action for invasion of privacy. This is the preferred outcome expressed by the majority of those that support the enactment of a statutory cause of action. It will also mean that the scope of the *Privacy Act* is broader than simply data protection, and therefore reflects more accurately the title of the Act. This is discussed in greater detail in Chapter 3.

---

146 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

147 For a discussion of the power of a court to grant a stay, see *Walton v Gardiner* (1993) 177 CLR 380, 392–393; S Odgers, *Uniform Evidence Law* (6th ed, 2004), [1.1.1240]–[1.1.1260]. For a discussion of the complaint handling powers of the OPC, see Ch 45.

5.108 Further, as is evidenced by the Preamble to the *Privacy Act*, and discussed in Chapters 1 and 3, the *Privacy Act* partially implemented into domestic law Australia's obligations under art 17 of the ICCPR. Locating the statutory cause of action in the Act essentially fulfils Australia's international obligations arising under art 17.[148]

5.109 Whether the appropriate forum to bring the action is the state and territory or federal courts is a related, but separate, question. Locating the cause of action in federal legislation does not preclude state courts from hearing such matters. The use of state courts to hear federal matters is made possible by ss 71 and 77(iii) of the *Australian Constitution*. Section 71 vests the judicial power of the Commonwealth in the High Court, in such other federal courts as the Australian Parliament creates, and in such other courts as it invests with federal jurisdiction. Section 77(iii) provides that the Australian Parliament may make laws investing state courts with federal jurisdiction. Section 39(2) of the *Judiciary Act 1903* (Cth) invests state courts with federal jurisdiction in both civil and criminal matters, subject to certain limitations and exceptions.

5.110 The appropriate court to hear the action will depend on the circumstances giving rise to liability, and the nature and extent of the remedies claimed. If the cases brought to date in Australia are any guide, it is likely that the District/County Court will be the most appropriate forum given the scope of its jurisdiction, the cost of litigating in that court, and the expertise of the judges in hearing comparable matters, such as tort actions.

Limitations on the statutory cause of action

5.111 If a statutory cause of action for invasion of privacy is enacted, what limitations should apply? For example, who should be permitted to bring the action? Should the cause of action be restricted to intentional invasions of privacy, or should it also include reckless, negligent or accidental acts? Is proof of damage a prerequisite to bringing the cause of action? All of these issues are canvassed in some detail in NSWLRC CP 1,[149] and therefore will be discussed only briefly here.

Who should be permitted to bring the action?

5.112 It was suggested by two members of the High Court in *Lenah Game Meats* that the development of an emergent tort of invasion of privacy should benefit natural, not artificial, persons.[150] This accords with the ALRC's view in this Inquiry that the *Privacy Act* should not be amended to provide direct protection for corporate entities or groups.[151] Based on the reasoning set out in detail in Chapter 1, the ALRC's view is

148 While Proposal 5–1 does not list 'unlawful attacks on honour and reputation' as an actionable element, as is noted above, protection from such attacks is already adequately provided for in domestic defamation law.

149 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), Ch 7.

150 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [132] (per Gummow and Hayne JJ).

151 See Ch 1.

that the statutory cause of action for invasion of privacy should benefit individuals, not corporations, unincorporated commercial entities or groups.

Intentional, reckless, negligent and accidental acts

5.113 An act is intentional when the defendant deliberately or wilfully invades the plaintiff's privacy. The meaning of 'reckless' was discussed by Diplock LJ in the criminal case of *R v Caldwell*:

> 'Reckless' … is an ordinary English word. It had not by 1971 [the year the *Criminal Damage Act* considered in the case came into force] become a term of legal art with some more limited esoteric meaning than that which it bore in ordinary speech, a meaning which surely includes not only deciding to ignore a risk of harmful consequences resulting from one's acts that one has recognised as existing, but also failing to give any thought to whether or not there is any such risk in circumstances where, if any thought were given to the matter, it would be obvious that there was.[152]

5.114 The Law Reform Commission of Hong Kong, in recommending a cause of action for intrusion into the solitude, seclusion or private affairs of another person, rejected the suggestion that a plaintiff should be allowed to recover for accidental or negligent intrusions. It was, however, of the view that liability should lie for reckless intrusions.

> Since indifference to the consequences of an invasion of privacy is as culpable as intentionally invading another's privacy, we consider that an intrusion must be either intentional or reckless before the intruder could be held liable.[153]

5.115 The NSWLRC suggests that 'including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[154] The ALRC agrees, and suggests that the fault element of the cause of action for invasion of privacy should be restricted to intentional or reckless acts on the part of the defendant.

Proof of damage

5.116 The statutes of British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador providing for the tort of violation of privacy, and the Privacy Bill currently before the Irish Parliament, all provide that the tort of violation of privacy is actionable without proof of damage. In other words, the cause of action is actionable *per se*—there is no requirement on the plaintiff to prove that any actual damage arose from the invasion of privacy.

5.117 In this regard, the tort of invasion of privacy differs from the tort of negligence, in that proof of damage is an essential element of the latter. The treatment of the tort of

---

152 *R v Caldwell* [1981] 1 All ER 961, 966.
153 Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy* (2004), [6.71].
154 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), [7.24].

invasion of privacy is, therefore, more akin to trespass to the person or defamation, which are actionable without proof of damage.

5.118 Providing that the proposed cause of action for invasion of privacy is actionable without proof of damage will allow for an award of compensation for insult and humiliation.[155] It will also allow the court to award a wider range of remedies to address the invasion—for example, an order requiring the defendant to apologise to the plaintiff.

5.119 Finally, providing that invasion of privacy is actionable without proof of damage is itself recognition that the cause of action protects a fundamental human right. A breach of such a right should not be dependent on proof of damage flowing from the breach.[156]

Proposal 5–1 The *Privacy Act* should be amended to provide for a statutory cause of action for invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, an invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

Proposal 5–2 The *Privacy Act* should provide that, in determining what is considered 'private' for the purpose of establishing liability under the proposed statutory cause of action, a plaintiff must show that in all the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities.

Proposal 5–3 The *Privacy Act* should provide that:

(a) only natural persons should be allowed to bring an action under the *Privacy Act* for invasion of privacy;

155 F Trindade and P Cane, *The Law of Torts in Australia* (3rd ed, 1999), 23.

156 For a discussion of the status of privacy as a human right, see Ch 1.

(b) the action is actionable without proof of damage; and

(c) the action is restricted to intentional or reckless acts on the part of the defendant.

Proposal 5–4 The Office of the Privacy Commissioner should provide information to the public concerning the proposed statutory cause of action for invasion of privacy.

Proposal 5–5 The range of defences to the proposed statutory cause of action for invasion of privacy provided for in the *Privacy Act* should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or specifically authorised by or under law;

(c) information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

(d) disclosure of the information was, under the law of defamation, privileged.

Question 5–1 In addition to the defences listed in Proposal 5–5, are there any other defences that should apply to the proposed statutory cause of action for invasion of privacy?

Proposal 5–6 To address an invasion of privacy, the court should be empowered by the *Privacy Act* to choose the remedy that is most appropriate in all the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law. For example, the court should be empowered to grant any one or more of the following:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the defendant to apologise to the plaintiff;

(e) a correction order;

(f) an order for the delivery up and destruction of material;

(g) a declaration; and

(h) other remedies or orders that the court thinks appropriate in the circumstances.

Proposal 5–7 Until such time as the states and territories enact uniform legislation, the state and territory public sectors should be subject to the proposed statutory cause of action for invasion of privacy in the *Privacy Act*.

6. Overview—Impact of Developing Technology on Privacy

Contents

Introduction	311
Privacy enhancing technologies	312
Encryption	313
Identity management	314
The internet	315
Data collection on the internet	316
Security of the internet	319
Internet of things	320
Radio frequency identification	321
Other wireless technologies	325
Data-matching and data-mining	325
Smart cards	327
Biometric technologies	330
DNA-based technologies	333
Voice over internet protocol	334
Location detection technologies	335
Surveillance technologies	337
Other developing technologies	339

Introduction

6.1 Developments in technology have always influenced discussions about privacy and the development of information privacy laws. The first modern academic discussion of privacy in 1890[1] was prompted by concerns at that time about the impact of new technologies on privacy, in particular 'instantaneous photography'.[2] In 1983, concerns about dangers to privacy, including developments in information technology and surveillance technology, led the ALRC to recommend that legislation containing information privacy principles be introduced.[3] In the second reading speech for the Privacy Bill 1988 (Cth) the then Attorney-General, the Hon Lionel Bowen MP, stated that rapid developments in technology for the processing of information had 'focused attention on the need for the regulation of the collection and use of personal

1 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
2 D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 10.
3 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Rec 58.

information by government agencies and for an independent community spokesperson for privacy'.[4] In 2000, concerns about the security of personal information disclosed during online transactions provided impetus for the introduction of the private sector provisions of the *Privacy Act 1988* (Cth).[5]

6.2 Two recent reviews have considered privacy and emerging technologies. In 2005, the Office of the Privacy Commissioner (OPC) concluded a review of the private sector provisions of the *Privacy Act* (OPC Review) and the Senate Legal and Constitutional References Committee concluded an inquiry into the *Privacy Act* (Senate Committee privacy inquiry). Both the OPC and the Senate Committee recommended that there should be a wider review of privacy laws in Australia and that this review should consider whether the provisions of the *Privacy Act* remained adequate and effective in light of developments in technology.[6]

6.3 Part B of this Discussion Paper considers the impact of developing technology on privacy. This chapter provides an overview of several developing technologies. Chapter 7 discusses how best to accommodate developing technology in a regulatory framework. The impact of Web 2.0 and how the internet has changed the nature of a 'public' space are discussed in Chapter 8.[7] Finally, Chapter 9 discusses the prevalence of identity theft in an electronic environment.

Privacy enhancing technologies

6.4 Some technologies known as privacy enhancing technologies (PETs) operate to protect privacy. The way that technology is used often determines whether it is privacy enhancing or privacy invasive.[8] Particular PETs that can be implemented by individuals are discussed throughout this chapter.[9] It is important to note, however, that agencies and organisations should be encouraged to incorporate PETs into technical systems at the design stage. For example, the United States National Security Agency and members of the IT industry are developing a system that implements a mandatory access control (MAC) framework that provides enforced security settings and prevents the setting of discretionary preferences by a computer application or user.[10] Two other

---

4 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General), 2118.

5 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15749.

6 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), recs 6, 8; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 1, 69.

7 The term 'Web 2.0' can be used in various contexts. In this Discussion Paper, it is used to refer to the social phenomenon where internet users—often individuals acting in a personal capacity—upload and distribute content such as text, photographs and videos.

8 See, eg, J Alhadeff, *Consultation*, Sydney, 26 April 2007; M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002), 9–10.

9 The role of PETs in a regulatory framework is discussed in Ch 7.

10 United States National Security Agency, *Security-Enhanced Linux* (2007) <www.nsa.gov/selinux/> at 30 July 2007.

PETs that can be used in the online environment are encryption and identity management, considered in more detail below.

Encryption

6.5 Encryption, a form of cryptography, refers to a sequence of processes that ensure that information stored in electronic form or transmitted over networks such as the internet is not accessible to any person not authorised to view that information. Encryption can be used to convert data to a form which cannot be read without using an appropriate 'key'. A particular form of encryption, public-key cryptography, enables the creation and use of 'digital signatures'—that is, the encryption of data in a message with a private key allocated to a particular sender that assures others that only the sender could have created the message.[11] Encryption does not, however, prevent the deletion of information.

6.6 Encryption systems use either, or both, symmetric or asymmetric key ciphers. Information encoded by a symmetric key cipher requires the decoder of the message to hold a key that is identical to, or readily derived from, the key held by the encoder. An asymmetric key cipher system, such as public-key cryptography, uses a combination of a secret 'private' key and a widely available 'public' key. In this system, information encoded using the public key remains encrypted and secure until a person holding the corresponding private key receives the information and uses the private key to decode the information. In some asymmetric systems, the private key can also be used to encode information so that the corresponding public key can be used to decode the information. This reverse approach provides a 'guarantee of authenticity' rather than an encryption method as any person can decode the information using a public key.[12] In comparison to symmetric key cipher systems, asymmetric systems are complex and slow in execution.[13]

6.7 Symmetric and asymmetric encryption systems can be used in conjunction with mechanisms such as one-way-hash functions to ensure that information stored or transmitted in an encrypted form remains unaltered. A hash function can be applied to data, or a message, to produce data of a fixed bit length—for example, 8, 16 or 32 characters. The hash function condenses the message to a 'hash value' of the original message. In a security system intended to safeguard the integrity of messages against any alteration, a hash value together with an original message is transmitted to a receiver who knows the relevant hash function. The receiver can apply the hash function to the original message to create a second hash value that may be compared against the original hash value. Identical hash values indicate that the original message

---

11 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), [2.77]–[2.113].

12 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 221.

13 United States Department of Commerce—National Institute of Standards and Technology, *Introduction to Public Key [Technology and the Federal PKI Infrastructure]* (2001), 11.

was not altered in transmission. The message, however, could have been intercepted, altered and a new hash value calculated and added. To prevent this, the hash value may itself be encrypted before being added to the message for transmission. A receiver who possesses a corresponding cipher key can then decrypt the hash value and compare it against a second hash value that is recalculated from the received message.[14]

Identity management

6.8 The remote nature of online transactions has led many agencies and organisations to require individuals to authenticate routinely their identity during transactions. Arguably, however, it is not always necessary for individuals to identify themselves when engaging in online transactions and it is more desirable for some forms of transactions to be 'pseudonymous'.[15] Pseudonymous transactions could be achieved through the use of 'identity escrow'—that is, a system where a trusted third party holds evidence about a person's identity and issues that person an identifier enabling him or her to conduct transactions with other parties.[16] Identity management systems are another measure that could facilitate the use of pseudonyms and partial identities.

6.9 Identity management systems provide a mechanism for establishing trust between individuals, agencies and organisations transacting in the online environment.[17] The Privacy Identity Management for Europe (PRIME) project, for instance, emphasises the privacy enhancing nature of its identity management project, noting that it allows individuals to minimise the disclosure of their personal information in the online environment and provides individuals with technical tools to negotiate privacy preferences with online entities.[18]

6.10 Identity management has been described as a three step process. First, an identity is established by a process of verification, which may require an individual to choose a password or verify his or her identity in person. Before using an identity, authentication through the presentation of credentials is required. A credential may be something that an individual *has*, such as a radio frequency identification (RFID) tag; something that an individual *knows*, such as a password; or something that an individual *is*, such as a facial biometric or fingerprint.[19] Finally, revocation of identity refers to the removal of an identity when use of that identity is no longer required, such

14 Y Fen Lim, *Cyberspace Law: Commentaries and Materials* (2nd ed, 2007), 221.
15 Proposal 17–1.
16 See, eg, R Clarke, *Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue* (1996) Australian National University <www.anu.edu.au/Roger.Clarke/DV/AnonPsPol.html> at 30 July 2007.
17 Information Integrity Solutions, *Trust and the Critical Role of User Centric ID Management* (2006), 1.
18 Privacy and Identity Management for Europe (PRIME), *PRIME White Paper v2* (2007), 1.
19 Information and Privacy Commissioner of Ontario and A Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (2007) Information and Privacy Commissioner of Ontario, 2.

as where a customer changes banks. Revocation of identity is an important measure to reduce identity theft.[20]

6.11 User-centric authentication systems require both an individual and the entity with which the individual is transacting to authenticate their identities. Such mutual authentication projects have emerged as a response to the 'asymmetric sharing of control … [that] commonly leads to a corresponding asymmetry of risk allocation' in the one-way trust model.[21] Microsoft and IBM have both developed user-centric identity management systems.[22]

6.12 A new trend in identity management is the development of the federated identity system.[23] Identity federation systems use a central identity provider to authenticate an individual, who can then access certain other domains without needing to re-authenticate their identity. In an identity federation system, individuals can manage their identities by setting pseudonyms for use in different domains and determining what information can be revealed in different contexts. Standardisation in identity federation systems is required for their effective operation, and this is currently the subject of deliberation in international forums.[24]

The internet

6.13 The internet is a worldwide collection of interconnected computer networks based on a set of standard communication protocols. The World Wide Web (the Web)—a global collection of publicly accessible electronic information—is accessed by individual computer 'nodes' that are attached to the internet. Individual computer nodes could be, for example, a personal computer (PC) or a wireless device such as a mobile phone. The internet was created in the mid 1980s and widespread use of it commenced in the 1990s. In 2006, surveys conducted by the Australian Bureau of Statistics indicated that 66% of Australians aged over 15 had accessed the internet within the past 12 months.[25]

---

20 International Telecommunication Union, *digital.life: ITU Internet Report 2006* (2006), 114. Identity theft is discussed in Ch 9.

21 Information Integrity Solutions, *Trust and the Critical Role of User Centric ID Management* (2006), 2.

22 Kim Cameron's '7 Laws of Identity' have been incorporated into Microsoft's 'CardSpace' application: K Cameron, *The Laws of Identity* (2005) Microsoft Corporation; Microsoft Corporation, *Introduction to Windows CardSpace* (2006) <cardspace.netfx3.com/content/introduction.aspx> at 30 July 2007. See too IBM, *Idemix: Pseudonymity for e-Transactions* (2006) <www.zurich.ibm.com/security/idemix/> at 30 July 2007.

23 S Wilson, *Correspondence*, 23 April 2007.

24 International Telecommunication Union, *digital.life: ITU Internet Report 2006* (2006), 115–120. In Chapter 7, the ALRC proposes that the *Privacy Act* be amended to empower the appropriate Minister to determine privacy and security standards.

25 Australian Bureau of Statistics, *8146.0—Household Use of Information Technology, Australia, 2005–2006* (2006).

6.14 The internet can be used for a myriad of social, economic and political transactions. It can be used by individuals to send and receive messages that include text, images and sound (email). It can also be used by individuals and organisations to engage in trade (e-commerce) or to advertise or promote goods or services (e-marketing). Further, it can be used by individuals to communicate with governments and access government services (e-government); to engage in leisure activities, such as online gaming; or to access information for personal purposes. It has been noted that user-generated content (or 'Web 2.0') sites such as MySpace, Facebook, Second Life, LinkedIn and YouTube are increasingly used by individuals for the dissemination of information and social and professional networking purposes.[26] Increasingly, social, business and political communications take place through user-generated sites, internet chatrooms, webcams and two-way videoconferencing.

Data collection on the internet

6.15 Currently, vast amounts of data are collected about internet users, often without their knowledge or consent. For example, data are often collected about the search terms an internet user has entered into an online search engine; the websites an internet user has visited; and the goods or services an internet user has purchased or enquired about online.[27] Data are also collected about internet users who use tools provided by online search engines, such as free email and map services.[28] These data have the potential to reveal a substantial amount of information about an internet user, including 'information about health, education, credit history, [and] sexual or political orientation'.[29] Information collected about internet users is not usually linked directly to an individual, but rather to a particular computer. This is because each computer connected to the internet is allocated a unique Internet Protocol (IP) address for the duration of each internet session.[30] Some information collected on the internet may be subject to the proposed Unified Privacy Principles (UPPs).[31]

6.16 Information collected about internet users can be used for a variety of purposes, such as to create a profile of the individual for marketing purposes. In 2004, 62% of respondents to research conducted for the OPC indicated that they had more concerns about their privacy than usual when using the internet.[32] Two in three respondents indicated that they had more concerns about their privacy when using the internet than they did two years previously.[33] This section provides a brief overview of the way in which data about internet users can be collected.

---

26 See, eg, Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007; B Howarth, 'Another Life', *Australian IT* (online), 3 April 2007, <www.australianit.news.com.au>.

27 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 113.

28 See, eg, A Brown, 'Google is Watching …', *The Age* (Melbourne), 2 September 2006, Insight 3.

29 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 114.

30 G Greenleaf, 'Privacy Principles—Irrelevant to Cyberspace?' (1996) 3 *Privacy Law & Policy Reporter* 114, 115.

31 See Proposal 3–5 and accompanying text.

32 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), [10.2].

33 Ibid, [10.2].

Cookies

6.17 A 'cookie' is a piece of information that is sent from a computer or website to an internet user's browser. The browser stores the information on the internet user's computer. If the user accesses the same website at a later time, the cookie is sent back from the user's computer to the website, thereby indicating that the same user has returned to the same website.

6.18 Cookies are used for a number of purposes, such as to personalise online search engines and store lists of items to be purchased online. Although cookies are principally linked to computers, they can also be linked to an individual in certain circumstances. For example, a cookie could be linked to an individual user if the user provides identifying details, such as his or her name and address, when browsing a website.

6.19 Cookies are often stored on an internet user's computer, and accessed by websites visited by the user, without the user's knowledge or consent. In addition, cookies can in some circumstances have a lifespan of several years. It is possible, however, for an internet user to take steps to prevent cookies being stored on his or her computer. For example, if the user's operating system allows it, he or she can limit the lifespan of cookies so that they are only stored for as long as the user's browser is running. Alternatively, an internet user can purchase and install software to assist the user to control the use of cookies when he or she enters the online environment.

Web bugs

6.20 A web bug is a small, invisible image that is included on a web page or email. When a web page containing a web bug is accessed, the web bug collects certain information, such as the IP address of the computer, the time the web page was accessed, and the type of browser used to access it. Web bugs are often used on web pages by third parties, such as advertisers, to track the web pages accessed by users. It has been noted that virus scanners have mixed success in locating web bugs on web pages as it is impractical to scan every web page that is accessed by a user.[34]

6.21 When an email containing a web bug is opened, the sender of the email is informed that the email has been opened and the time at which it was opened. In addition, web bugs can identify the IP address of the computer that opened the email. Web bugs can be used by marketers and 'spammers' to verify the validity of email addresses, or by individuals wishing to be informed of the number of times their email has been forwarded and read.[35]

---

34 W Caelli, *Correspondence*, 2 April 2007.

35 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 118.

Hypertext transfer protocol

6.22 Hypertext transfer protocol (HTTP) is a set of rules developed to enable information to be requested and sent on the Web. In order to access a particular web page, an internet user's browser must first request certain information. For example, it must send information about the Uniform Resource Locator (URL) of the web page that the user wishes to access. Further information can also be sent during the request for information, however, or the last web page viewed by the user.[36] If the last web page viewed by the user was an online search engine, then the search term entered is also transmitted.[37] In addition, it is possible for the identity of the user to be disclosed if the user's internet service provider (ISP) does not take steps to prevent this from happening.[38]

Spyware and remote access software

6.23 Software such as remote access software or spyware installed on a computer can enable a third party to view the activity or data on that computer.[39] Remote access software can be used for beneficial purposes, for example, by an employee in an organisation to fix another employee's computer from another location. Software that allows remote access to computers is not inherently harmful. On the other hand, spyware can be installed without the knowledge or consent of the user of the computer for malicious purposes, such as to collect personal information about the user for the purpose of engaging in fraudulent activities.

6.24 Spyware can be installed on a computer in a number of ways. For example, it can be physically installed by another individual, or installed in the online environment where it may be attached to an email or to downloaded material. In 2005, the Department of Communications, Information Technology and the Arts announced the outcome of a review of spyware. It concluded that the most serious and malicious uses of spyware were adequately addressed by existing laws, such as computer offences in the *Criminal Code* (Cth).[40]

Social engineering

6.25 Social engineering practices, such as pretexting or phishing, rely on a person providing information to another person, whether face-to-face or over the telephone or over the internet. Social engineering involves 'human interaction (social skills) to

---

36 Office of the Privacy Commissioner, *Protecting your Privacy on the Internet* <www.privacy.gov.au/internet> at 30 July 2007.

37 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 119.

38 Ibid, 119.

39 Australian Government Department of Communications Information Technology and the Arts, *Spyware Discussion Paper* (2005), [2.2.2].

40 Australian Government Department of Communications Information Technology and the Arts, *Outcome of the Review of the Legislative Framework on Spyware* (2005), [2.3].

obtain or compromise information about an organization or its computer systems'.[41] Phishing is discussed further in relation to identity theft in Chapter 9.

Security of the internet

6.26 There is concern about the security of personal information transmitted via the internet, particularly the security of information disclosed during the course of e-commerce. Such information may be intercepted during transmission or accessed in an unauthorised manner when stored electronically. Shortcomings in internet security have prompted research projects such as the 'Clean Slate Program' at Stanford University, which aims to design a new internet that is robust, predictable and 'inherently secure'.[42] This section focuses on internet and computer security. It should also be noted, however, that other technologies—such as wireless networks—have security risks that present significant privacy implications.[43]

6.27 A number of reports suggest that data thieves are increasingly 'hacking' into computer systems.[44] There are a number of ways that hackers can access personal information transmitted over the internet or stored on computer systems. For example, a hacker may infect a computer with spyware that can collect personal information displayed on a computer screen or stored on a computer system.[45] More sophisticated hacking techniques include the use of 'rootkits', which can be installed directly in an operating system kernel or system hardware and take over an entire computer system.[46] Rootkits have been described as 'cloaking technologies' since they can operate with other malware to hide 'files, registry keys and other operating system objects from diagnostic, antivirus and security programs'.[47]

6.28 Rootkits can be used to establish 'botnets', which are automated crime networks controlled by 'botherders' who use malware to infect numerous computers. Botnet computers are referred to as 'zombies' because a user of an infected computer generally is unaware that the computer has become part a botnet. Zombies can be used

---

41 United States Computer Emergency Readiness Team (US-CERT), *National Cyber Alert System—Avoiding Social Engineering and Phishing Attacks* (2004) <www.us-cert.gov/cas/tips/ST04-014.html> at 30 July 2007.

42 N McKeown and B Girod, *Clean-Slate Design for the Internet—A Research Program at Stanford University: Whitepaper Version 2.0* (2006) Stanford University, 2–3.

43 See, eg, R Naraine, *Wi-Fi Hacking, with a Handheld PDA* (2007) ZDNet <blogs.zdnet.com> at 6 February 2007; D Goodin, 'Flash: Public Wi-Fi Even More Insecure than Previously Thought', *The Register* (online), 2 August 2007, <www.theregister.co.uk>.

44 See, eg, 'The Year Hacking Became a Business', *Australian IT* (online), 30 January 2007, <www.australianit.news.com.au>; J Evers, 'Homeland Security Sees Cyberthreats on the Rise', *CNET News.com* (online), 8 February 2007, <news.com.com>.

45 W Caelli, *Correspondence*, 2 April 2007.

46 D Fisher, 'Rootkit Dangers at an 'All-time High'', *SearchSecurity.com* (online), 6 February 2007, <searchsecurity.techtarget.com>.

47 Australian Institute of Criminology, *High Tech Crime Brief No 12, 2006—High Tech Crime Tools*, 1 December 2006.

by botherders to carry out phishing and spam attacks and, ultimately, identity theft. The FBI has arrested a number of botherders in the United States. Botherders operate in several nations, however, and effective policing of botnets depends on inter-jurisdictional cooperation.[48]

6.29 Individuals are often advised to use commercially-available programs such as anti-virus and anti-spyware programs to ensure computer and network security.[49] It has been noted, however, that market-based solutions may not provide adequate protection against hackers.[50] Moreover, an online safety study conducted in the United States in 2004 indicates that many individuals incorrectly assume that their anti-virus protection is adequate and up-to-date.[51]

6.30 In Chapter 7, the ALRC proposes that the *Privacy Act* be amended to empower the appropriate minister to determine relevant privacy and security standards. Such standards could require that technical systems meet certain security requirements before they are marketed to individuals, agencies and organisations. Further, the ALRC proposes in Chapter 47 that the *Privacy Act* be amended to require agencies and organisations to notify the OPC and any affected individuals of data breaches in certain circumstances.[52] This measure is intended to reduce the likelihood of security breaches that may lead to identity theft.

Internet of things

6.31 The United Nations agency for information and communications technologies, the International Telecommunication Union, has predicted that the next development in information transfer will be the 'internet of things'. The internet of things, or ubiquitous computing, will allow the transfer of information between inanimate objects, humans, the internet, intranets and peer-to-peer networks—without the need for personal computers.[53] The internet of things will use wireless technologies such as RFID, which is discussed below, together with smart and sensor technologies and miniaturising technologies such as nanotechnology.[54]

6.32 The internet of things will be based on next generation networks (NGNs), which use 'packet-based' Internet Protocol (IP) Technology. Many telecommunications devices currently use the Public Switched Telephone Network (PSTN), which is a 'circuit-switched' network. In NGN networks, linked devices are more mobile than in

---

48 See, eg, 'FBI Tackles "Zombie" PC Networks', *Sydney Morning Herald* (online), 17 June 2007, <www.smh.com.au>.

49 See, eg, Australian Government, *Securing Your Computer* (2007) Australian Government Department of Communications, Information Technology and the Arts <www.staysmartonline.gov.au/securing_your_computer> at 30 July 2007.

50 P Croll and W Caelli, *Consultation PC 88*, Brisbane, 13 February 2007.

51 America Online and National Cyber Security Alliance, *AOL/NCSA Online Safety Study* (2004).

52 See Proposal 47–1. Identity theft is discussed in Ch 9.

53 International Telecommunication Union, *The Internet of Things* (2005), 3.

54 For an overview of nanotechnology, see S Wood, R Jones and A Geldart, *Nanotechnology: From the Science to the Social—A Report for the Economic and Social Research Council* (2007) Economic and Social Research Council.

PSTN networks, and service delivery is not linked to the underlying transport technologies.[55]

6.33 The internet of things could impact on privacy by allowing more information to be collected from an individual without his or her knowledge or consent. In addition, the convergence of technologies in the internet of things means that individuals could be more easily tracked, monitored and profiled.[56] It has also been noted that remote access to sensor networks could impact on security of information, as data thieves could 'collect information from further away and from multiple locations simultaneously'.[57] The European Commission is monitoring these developments and at the end of 2008 intends to issue to the European Parliament a communication on privacy, trust and governance issues related to the internet of things.[58]

Radio frequency identification

6.34 An RFID system consists of a 'transponder', a 'reader' and a 'back office' system. A transponder is a small object—often referred to as an 'RFID tag'—that transmits data by emitting radio waves.[59] These data are collected by a device known as a reader. Readers can be mobile, resembling hand-held barcode scanners, or fixed at certain locations, such as the entrance to a warehouse or a vehicle toll gateway.[60] Once data are collected by a reader they are sent to a 'back office'—namely, a data processing system.[61] In June 2006, BP commenced a 'mesh network' trial in which RFID tags or 'nodes' communicated information directly to other RFID tags. In this trial, an RFID node transmitted 'details of its environment and content … to all other nodes within a 3-meter range'.[62]

6.35 There are two main types of RFID tags—passive tags and active tags.[63] Passive tags lack an internal power source and can only operate if they are in range of a reader

---

55 International Telecommunication Union, *The Internet of Things* (2005), 4.

56 Ibid, 82–3.

57 Ibid, 83.

58 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 11.

59 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

60 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [1.1.2].

61 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

62 J Collins, 'BP Tests RFID Sensor Network at UK Plant', *RFID Journal* (online), 21 June 2006, <www.rfidjournal.com>.

63 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [1.1.1].

that activates the tag.[64] Accordingly, they have a limited 'read range'. They are relatively inexpensive, however, and have a longer life-cycle than active tags.[65] Active tags have an internal power source (usually a battery) that allows them to emit radio waves.[66] These radio waves can be read if the tag is in range of a reader. The 'read range' of active tags is much greater than that of passive tags (up to several kilometres).[67] Active tags also have larger amounts of memory and better processing capabilities than passive tags.[68]

6.36 RFID tags can be attached to objects, such as clothes, shopping trolleys or plastic cards. They can also be attached to animals and people. Passive tags are usually physically smaller than active tags and can be difficult for an individual to detect. An RFID tag can transmit data that identifies the object or entity to which it is attached, such as an unique serial number. It can also transmit data about the price, expiry date, colour, or date of purchase of a product.[69] If an RFID tag is combined with a sensor, it can also transmit data about its surroundings, such as the temperature in its location or the composition of the atmosphere surrounding it.[70]

6.37 RFID technology has been in existence since the 1940s.[71] Currently, it has a number of established uses, including facilitating automated payments at vehicle toll booths, enabling people to lock and unlock cars remotely, and enabling people to access secure buildings.[72] Additional uses for RFID technology are being deployed as the cost of the technology decreases.[73] In October 2004, the United States Food and Drug Administration approved the use of a subdermal RFID tag for medical purposes, such as to enable health service providers to obtain identity and health information relating to unconscious patients.[74] It has been predicted that between 2006 and 2016 the value of the RFID market will rise from $2.77 billion to $26.23 billion.[75]

---

64 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

65 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [2.1].

66 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

67 M Ward, R van Kranenburg and G Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) Joint Information Systems Committee Technology and Standards Watch, [2.1].

68 Ibid, [2.1].

69 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

70 Australian Government Department of Communications Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 6.

71 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

72 Ibid, 7; Australian Government Department of Communications Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 4.

73 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7. See also Hitachi, *World's Smallest and Thinnest 0.15 x 0.15 mm, 7.5μm Thick RFID IC Chip* (2006) <www.hitachi.com/New/cnews /060206.html> at 30 July 2007.

74 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.133]–[3.143].

75 IDTechEx, *RFID Market $2.77Bn in 2006 to $12.35Bn in 2010* <www.idtechex.com> at 30 July 2007.

6.38 The use of RFID technology can benefit businesses, individuals and governments. RFID technology can benefit individuals in the areas of safety, convenience and accessibility. For example, RFID can be used to trace food, lead to shorter supermarket queues and track patients suffering from Alzheimer's disease.[76] It may also be used by businesses to track products from the point of manufacture to the point of sale, thereby reducing inventory and labour costs, and stock losses.[77] Other applications of RFID technology include:

> prevention of counterfeiting of consumer goods; pinpointing the location of theft; library book check-out; tracking passenger bags in airports; residential garbage collection; sensitive document tracking; asset management; equipment and personnel tracking in hospitals; parcel and post management; livestock management; inmate and guard tracking systems for prison security management; parking permits; tire pressure monitoring; and pharmaceutical labelling for monitoring of location, expiration and anti-counterfeiting.[78]

6.39 It has also been suggested that RFID technology could be used to create 'smart products', such as washing machines that wash garments in accordance with instructions on their RFID tags.[79]

6.40 Some uses of RFID technology raise privacy concerns. In particular, concerns arise about the ability of agencies, organisations or individuals to

> surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; [and] read the details of clothes and accessories worn and medicines carried by customers.[80]

6.41 These concerns are exacerbated by the fact that individuals may not be given notice that the products they purchase or the objects they use contain RFID tags and may not be given the choice to remove or disable RFID tags. Further, they may not be able to ascertain when, or how many times, data on an RFID tag have been collected.[81] Technologies have been developed that aim to prevent the unwanted scanning of RFID tags, such as 'blocker tags' which 'impair readers by simulating the signals of many

---

76 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 3–4.

77 Australian Government Department of Communications Information Technology and the Arts, *Getting the Most out of RFID: A Starting Guide to Radio Frequency Identification for SMEs* (2006), 13–16.

78 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 307–308.

79 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 8.

80 European Union Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP105 (2005), [1].

81 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 5.

different RFID tags'.[82] An individual may not be aware, however, that a product contains an RFID tag and it may not be practical to purchase and carry an RFID blocker. It has been argued, therefore, that PETs are unable completely to 'assuage the danger to privacy engendered by RFID technology'.[83]

6.42 In 2002, one commentator proposed that organisations wishing to use RFID technology should comply voluntarily with an 'RFID Bill of Rights' that granted consumers the right to:

- know whether a product contained an RFID tag;
- have an RFID tag removed or deactivated at the point of purchase;
- use RFID-enabled services without RFID tags;
- access an RFID tag's stored data; and
- know when, where and why RFID tags are being read.[84]

6.43 To these, other commentators have added that consumers should have the right to:

- own and use readers that enable them to detect and permanently disable RFID tags;
- know who to contact in order to access information pertaining to them that has been collected by RFID technology; and
- the secure transmission and storage of data.[85]

6.44 In March 2007, the European Commission issued a Communication on RFID to the European Parliament, noting the need for legal certainty for both investors and users of RFID. The European Commission plans to establish a widely constituted RFID Stakeholder Group to discuss security and privacy issues with a view to issuing

---

82 Information and Privacy Commissioner Ontario, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (2004), 19. See also, Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 26; G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 315–320.

83 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 320.

84 S Garfinkel, 'An RFID Bill of Rights 1' (2002) 105(8) *Technology Review* 35, 35.

85 See Privacy Rights Clearinghouse, *RFID and the Public Policy Void: Testimony of Beth Givens, PRC Director to the California Legislature Joint Committee on Preparing California for the 21st Century* (2003) <www.privacyrights.org/ar/RFIDHearing.htm> at 30 July 2007.

at the end of 2007 a recommendation that sets out the principles that European public authorities and stakeholders should apply in respect of RFID usage.[86]

Other wireless technologies

6.45 Wireless technologies enable devices to transmit and receive data 'by means of a signal that uses some part of the electromagnetic spectrum'.[87] RFID technology, discussed above, is a wireless technology. 'WiFi' and 'Bluetooth' are examples of other wireless technologies.[88] WiFi technology enables devices to connect to the internet in certain 'hotspots', while Bluetooth technology enables devices to connect to each other across short distances.

6.46 Wireless technologies can be used to purchase goods, services or digital content (m-commerce), to enhance business performance (m-enterprise) and to provide services that do not involve commercial transactions, such as mobile banking services (m-services). Wireless devices such as personal digital assistants (PDAs) and mobile telephones are increasingly using similar hardware and software systems to those used in PCs. The use of wireless technologies raises privacy concerns because 'device limitations, along with different network configurations mean that wireless technologies present a higher risk from eavesdropping and hackers'.[89] Further, devices that use wireless technologies are vulnerable to theft and subsequent misuse.

Data-matching and data-mining

6.47 Rapid advances in information and communication technology since the 1970s have enabled agencies and organisations to collect and store vast amounts of personal information. This information is often generated by individuals conducting everyday activities, such as

> withdrawing cash from ATMs; paying with debit or credit cards; using loyalty cards; borrowing money; writing cheques; renting a car or a video; making a telephone call

---

86 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework* (2007), 4–11.

87 R Clarke, *Wireless Transmission and Mobile Technologies* (2003) Australian National University <www.anu.edu.au/people/Roger.Clarke/EC/WMT.html> at 30 July 2007.

88 The term 'WiFi' is commonly used to describe wireless local area networks based on a particular standard developed by the Institute of Electrical and Electronics Engineers (the IEEE 802.11 standard), while the term 'Bluetooth' is commonly used to describe wireless personal area networks based on the IEEE 802.15.1 standard. In June 2007, the Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, announced the implementation of a national wireless broadband network based on the IEEE 806.16d standard. Standards are discussed in Ch 7.

89 C Gould and others, 'Mapping the Mobile Landscape in Australia ' (2006) 11 *First Monday* <firstmonday.org/issues/issue11_11/gould/index.html>.

> or an insurance claim; and, increasingly, sending or receiving e-mail and surfing the Net.[90]

6.48 In addition, some technologies enable large amounts of personal information to be organised and analysed. Two methods of processing and analysing information are discussed in this section—data-matching and data-mining. This chapter discusses data-matching and data-mining outside the health and research context. A number of data-linkage models that provide for the linking of de-identified personal information for the purposes of health and medical research are discussed in Chapter 58.

6.49 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest'.[91] Developments in information technology in the 1970s made data-matching economically feasible and it is conducted regularly in Australia, particularly by government agencies.[92] Data-matching can be conducted for a number of purposes, including to detect errors and illegal behaviour, locate individuals, ascertain whether a particular individual is eligible to receive a benefit, and facilitate debt collection.[93]

6.50 Data-mining has been defined as 'a set of automated techniques used to extract buried or previously unknown pieces of information from large databases'.[94] Data-mining can be used in different contexts to achieve different goals. For example, it is increasingly used by organisations to enable them to 'design effective sales campaigns, precision targeted marketing plans, and develop products to increase sales and profitability'.[95] Data-mining can also be used by law enforcement agencies to investigate criminal activities. For example, in 2006 it was reported that the National Security Agency in the United States was collecting telephone records of millions of Americans to analyse calling patterns in an effort to detect terrorist activities.[96]

6.51 There are three main steps in the data-mining process: (1) the data are prepared (or 'scrubbed') for use in the data-mining process; (2) a data-mining algorithm is used to process the data; and (3) the results of the data-mining process are evaluated.[97]

6.52 Data-matching and data-mining practices that involve personal information raise a number of privacy concerns. A major concern is that the practices can reveal large

---

90 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 1.

91 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].

92 R Clarke, 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism' (1995) 4 *Information Infrastructure and Policy* 29, 30.

93 Ibid, 33.

94 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 4.

95 Ibid, 1.

96 L Cauley, 'NSA has Massive Database of Americans' Phone Calls', *USA Today*, 10 May 2006, <www.usatoday.com>.

97 J Bigus, *Data Mining with Neural Networks* (1996), 10–11, cited in Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 5.

amounts of previously unknown personal information about individuals.[98] This concern is exacerbated by the fact that data-matching or data-mining can occur without the knowledge or consent of the data subject, thereby limiting the ability of the data subject to seek access to information derived from a data-matching or data-mining program.[99]

6.53 Another concern relates to the accuracy of the data derived from a data-matching or data-mining process. Data-matching and data-mining involve using information collected for different purposes and in different contexts.[100] If information is incorrect or incomplete at the time of collection, or ceases to be accurate some time after collection, the information generated by the data-matching or data-mining process will be inaccurate. In the case of data-mining, an additional concern is that it is often difficult to inform the data subject of the exact purpose for which his or her personal information is to be collected or used. This is because data-mining activities aim to discover previously unknown information. Further, there is concern about the storage of large amounts of personal information gathered for the purpose of data-matching or data-mining.[101] In Chapter 7, the ALRC proposes that the OPC provide guidance on data-matching to organisations.

Smart cards

6.54 A smart card is usually a plastic card with an embedded microchip that can be programmed to perform multiple and varied functions.[102] A microchip embedded in a smart card can vary in sophistication.[103] Some microchips have memory functions only, while others have 'a micro-controller, various types of memory and an operating system'.[104] It has been noted that 'multi-application smartcards today have approximately the same capabilities and logical powers as the first commercial micro-computers in the mid 1970s'.[105]

6.55 Smart card technology has existed for several decades and has been described as 'technology looking for an application'.[106] Currently, smart card technology has a

98 V Estivill-Castro, L Brankovic and D Dowe, 'Privacy in Data Mining' (1999) 6 *Privacy Law & Policy Reporter* 33, 34.

99 See, eg, Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 14.

100 See, eg, Ibid, 10–11.

101 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

102 See, eg, S Newman and G Sutter, 'Electronic Payments—The Smart Card: Smart Cards, E-payments, & Law—Part I' (2002) 18 *Computer Law & Security Report* 235, 235; Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), i.

103 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006), [b.6].

104 Ibid, [b.6].

105 Ibid, [b.6].

106 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), 3.

number of established uses. For example, a Subscriber Identity Module (SIM) card in a mobile telephone uses smart card technology.[107] Smart cards also have a number of nascent uses, including for identity authentication and financial transactions. For example, a smart card could store a cardholder's biometric information in order to enable the cardholder to access a building or computer network. It could also contain an 'electronic purse' that can be used as a substitute for cash in small value transactions, such as for travel on public transport or small retail purchases.[108]

6.56 Smart cards can be divided into two main categories: 'contact smart cards' and 'contactless smart cards'. Information contained on a contact smart card can only be read if the card is inserted directly into a card reader. Contactless smart cards, however, use low-frequency radio waves to communicate with readers. Accordingly, they can be read from a distance.[109]

6.57 The use of smart card technology raises several privacy concerns. One concern is that a particular smart card may be linked to a particular individual, for example, where the individual uses his or her bank account to add value to the card's electronic purse. Widespread use of smart cards that are linked to identifiable individuals may mean that individuals no longer have the option of transacting anonymously.[110] Further, widespread use of these cards could enable vast amounts of information about the activities of cardholders to be collected and stored. In the future, smart cards could

> generate records of the date, time and location of all movements on public and private transport systems, along with details of all goods purchased, telephone use, car parking, attendance at the cinema, and any other activities paid for by smart cards.[111]

6.58 These records could then be used by smart card operators or third parties for a number of purposes, for example, to generate detailed profiles of individuals to market goods and services to them. They may also be sought by third parties, such as law enforcement agencies.[112]

6.59 Another concern is that smart card schemes that are used by numerous agencies or organisations may lack a central data controller. Accordingly, it may be unclear who is accountable for the use, disclosure, accuracy and security of personal information collected by the smart card system.[113] Concern has also been expressed about the potential for function creep[114] and the ability to read contactless smart cards without

---

107 S Newman and G Sutter, 'Electronic Payments—The Smart Card: Smart Cards, E-payments, & Law—Part I' (2002) 18 *Computer Law & Security Report* 235, 235.

108 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), i.

109 Council of Europe, *Report on the Protection of Personal Data with Regard to the Use of Smart Cards* (2001).

110 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), ii.

111 Ibid, ii.

112 Ibid, ii–iii.

113 Office of the Victorian Privacy Commissioner, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005, [26].

114 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.40], [3.43]–[3.54].

the cardholder's knowledge or consent. Finally, the security of a smart card system depends on the reliability and security of the various components of the system—that is, the security of the data pathways between the smart card and any reading, processing, storage or transmission system.

6.60 In 2004, the Council of Europe published a set of guiding principles for the protection of personal information in systems using smart card technology.[115] After acknowledging that the protection of personal information in any smart card system depended 'on many different factors and circumstances', the Council set out 11 principles to be taken into account by those who issue smart cards, as well as other participants in smart card systems, such as project designers and managers.

6.61 Among other things, the principles require the collection of personal information for storage on a smart card to be for 'legitimate, specific and explicit purposes'.[116] They also require a smart card to offer an appropriate level of security given the state of technology, the data stored on the card, the applications of the card, and the security risks.[117] Further, they require a data subject to be alerted every time personal information is exchanged between a smart card and a smart card system.[118]

6.62 In 2006, the Australian Government released part of a framework to assist agencies seeking to implement smart card technology.[119] The framework requires agencies implementing smart card technologies to include data protection clauses in agreements with third parties about the supply of smart cards and related services, and to undertake privacy impact assessments during the design of smart card systems. It also requires agencies implementing smart card technologies to produce comprehensive privacy policy statements and to revise these statements 'whenever a third party agency adds additional functionality to an existing smartcard deployment'.[120] In March 2007, the Australian Government released the final parts of the framework, the *Smartcard Implementation Guide* and *Standards and Model Specification*. At the time of writing in July 2007, the Australian Government is considering public comments on the proposed Smartcard framework.[121]

---

115 Council of Europe, *Guiding Principles for the Protection of Personal Data with Regard to Smart Cards* (2004).
116 Ibid, Principle 2.
117 Ibid, Principle 6.
118 Ibid, Principle 9.
119 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006).
120 Ibid, [a.17].
121 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2007) <www.agimo.gov.au/infrastructure/smart_cards> at 22 July 2007.

Biometric technologies

6.63 Biometric technologies enable unique behavioural or physiological attributes of people to be used for identification and authentication.[122] Major biometric technologies include finger scanning, facial recognition, iris and retinal scanning, finger geometry, voice recognition and dynamic signature verification.[123] Other biometric technologies include ear geometry, body odour measurement, keystroke dynamics and gait recognition.[124] Palm vein biometric systems are being developed for application in Automated Teller Machine (ATM) transactions.[125]

6.64 In a typical biometric system, a biometric device, such as a finger scanner, is used to take a biometric sample from an individual.[126] Data from the sample are then analysed and converted into a biometric template, which is stored in a database or an object in the individual's possession, such as a smart card.[127] Later biometric samples taken from the individual can then be compared to the stored biometric information to determine who the individual is (identification, or one-to-many matching) or to attempt to verify that an individual is who he or she claims to be (authentication, or one-to-one matching).[128] One-to-one systems currently provide higher accuracy of matches, although the accuracy of biometric systems varies greatly between systems.[129]

6.65 Biometric technologies have existed for decades.[130] The use of biometric technologies is increasing, however, because of globalisation, developments in information technology, and the desire to identify individuals in order to manage security threats such as terrorism.[131] Biometric systems enable the identification of an individual to be ascertained or authenticated with a fair degree of certainty. Further, advances in biometric technologies mean that biometric systems are now automated, allowing for 'mass identity checks within seconds … with a sufficient degree of certainty'.[132] For this reason, biometric technologies are increasingly used in

---

122 Biometrics Institute, *Biometrics Institute Ltd* <www.biometricsinstitute.org> at 31 August 2006; Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 10–11; Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [16].

123 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

124 Ibid, 4.

125 Fujitsu, *R&D—Fujitsu Palm Vein Technology* (2007) <www.fujitsu.com/global/about/rd/200506palm-vein.html> at 19 July 2007.

126 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

127 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [16]; Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

128 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.

129 See, eg, Y Wei Yun, *The '123' of Biometric Technology* (2002), 91–93.

130 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [8].

131 Ibid, [12].

132 Ibid, [8].

identification systems, along with other passwords or identity objects, such as smart cards.[133]

6.66 Since 2003, members of the European Union have been required to take fingerprints from all asylum seekers over the age of 14. These fingerprints are then compared to those in a centralised database to determine whether an asylum seeker has previously sought asylum in another Member State.[134] In addition, in 2003 the International Civil Aviation Organisation (ICAO) published 'a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs)'. The ICAO standards require MRTDs to include a facial image in a contactless chip.[135]

6.67 Biometric systems are also being introduced by the Australian Government. For example, in 2003 legislation was passed enabling officials to collect certain types of biometric information from non-citizens in Australia.[136] The legislation aims to ensure that non-citizens are identified accurately in order to enable officials to prevent identity fraud in the visa application process, to determine which non-citizens are of national security concern, and to detect forum shopping by visa applicants.[137] Further, in October 2005 the Australian Government introduced the 'ePassport'—a passport with an embedded microchip containing, among other things, a digitised facial image of the passport holder.[138] From 2007, those holding an ePassport will be able to use an automated border security system called 'SmartGate' in at least one airport in Australia. The SmartGate system will use facial recognition technology to perform the customs and immigration checks normally performed by Australian customs officers.[139] Australian ePassport holders will also be able to participate in the United States Visa Waiver Program.[140]

6.68 Biometric systems are being increasingly used or contemplated by organisations, including in methadone programs, taxi booking services, ATMs and online banking, and access to buildings.[141]

---

133 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–14.

134 European Commission, *EURODAC: The Fingerprint Database to Assist the Asylum Procedure* (2004).

135 International Civil Aviation Organization, *ICAO Recommendation* <mrtd.icao.int> at 30 July 2007.

136 *Migration Act 1958* (Cth) ss 5A, 40, 46, 166, 170, 172, 175, 188, 192.

137 Explanatory Memorandum, Migration Legislation Amendment (Identification and Authentication) Bill 2003 (Cth).

138 A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005).

139 Australian Customs Service, *SmartGate* (2006) <www.customs.gov.au/site/page.cfm?u=4243> at 4 September 2006.

140 United States Government Department of State, *Visa Waiver Program (VWP)* (2006) <travel.state.gov/visa/temp/without/without_1990.html> at 1 August 2007.

141 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

6.69 The use of biometric technologies raises a number of privacy concerns. These may vary according to the context in which the biometric information is collected and the type of biometric system in operation.[142] Some of the general concerns are as follows.

6.70 First, there is a concern that widespread use of biometric systems will enable extensive monitoring of the activities of individuals.[143] This is particularly so if the same form of biometric information is used to identify individuals in a number of different contexts—that is, if a type of biometric information is used as a unique multi-purpose identifier.[144] Secondly, there is a concern that biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent.[145] Thirdly, there is a concern that biometric information could reveal sensitive personal information, such as information about a person's health or religious beliefs.[146] Fourthly, there is a concern that the security of biometric systems could be compromised and that biometric information stored in a central or local database, or on an object in the possession of an individual, could be acquired by those wishing to use it for some kind of gain.[147] Finally, the accuracy and reliability of many biometric systems are still unknown,[148] causing some to express concern about the potentially serious consequences for an individual who is falsely accepted or rejected by a biometric system.[149]

6.71 The Council of Europe has cautioned that biometric systems should not be implemented for the mere sake of convenience.[150] It has recommended that before introducing a biometric system

> the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life.[151]

---

142 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

143 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12.

144 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002). Unique multi-purpose identifiers are discussed further in Ch 27.

145 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12–13.

146 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 6; M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).

147 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–15.

148 Ibid, 36.

149 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005); Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 10.

150 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [107].

151 Ibid, [107].

DNA-based technologies

6.72 It has been argued that DNA-based technologies differ from biometric technologies because they require actual physical samples to be taken from a person, as opposed to the taking of an image or scan of a person; and because DNA matching is not automated or done in real time.[152] The use of DNA-based technologies, however, raise a number of the same privacy issues as are raised by the use of biometric technologies.

Genetic samples

6.73 In 2003, the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council released *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96). The report was the product of a joint two-year inquiry into the legal and ethical issues surrounding human genetic information. In this report the ALRC and AHEC considered the privacy of human genetic samples, an issue that is discussed further below, and the privacy of human genetic information, which is discussed in Chapter 56.

6.74 ALRC 96 concluded that the *Privacy Act* did not cover genetic samples. This was because it was unlikely that genetic samples constituted 'information', or information stored in a 'record', for the purposes of the *Privacy Act*. Further, an unidentified and uncoded genetic sample might not constitute 'personal information' for the purposes of the Act.[153] Consequently these types of samples could be collected, stored and transferred with little or no regulation.

6.75 The ALRC and AHEC, therefore, recommended that the *Privacy Act* be amended to extend the coverage of the Information Privacy Principles (IPPs) and the NPPs to identifiable genetic samples. In particular, the ALRC and AHEC recommended that the definition of 'personal information' be amended to include bodily samples from an individual whose identity was apparent or could reasonably be ascertained from the sample, and that the definition of a 'record' be amended to include a bodily sample.[154]

6.76 The ALRC and AHEC also recommended that the *Privacy Act* be amended to provide that an individual had a right to access part of his or her own bodily samples, through a nominated medical practitioner, for the purpose of medical testing, diagnosis or treatment. Access could be refused in certain circumstances.[155]

---

152 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

153 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [8.4]–[8.26].

154 Ibid, Rec 8–2.

155 Ibid, Rec 8–3.

6.77 Finally, the ALRC and AHEC recommended that the *Privacy Act* be amended to enable an individual to access part of a bodily sample of his or her first-degree genetic relatives, through a nominated medical practitioner, where such access was necessary to lessen or prevent a serious threat to his or her life, health, or safety. An organisation subject to the *Privacy Act* that received such a request would be obliged to seek consent from the genetic relative, where practicable, before determining whether to provide access. Again, access could be refused in certain circumstances, including when it would have an unreasonable impact upon the privacy of the individual from whom the sample comes.[156] The Australian Government rejected these recommendations and, to date, they have not been implemented.[157] The ALRC does not propose to revisit these issues in the current Inquiry.

Voice over internet protocol

6.78 Voice over internet protocol (VoIP) enables spoken conversations to be conducted in real time over the internet.[158] It is a subset of technology referred to as 'IP Telephony', which enables facsimile messages, video and other forms of data traditionally transmitted via the Public Switched Telephone Network (PSTN) to be transmitted via the internet. IP telephony also enables the transmission of television and radio services.

6.79 VoIP technology transmits the sound waves of speech via the internet in the form of IP data packets.[159] It enables users to avoid the costs of communicating over long distances that are often incurred with traditional telecommunication carriers. It also enables users to encrypt telephone conversations and conduct telephone conversations with groups of people. VoIP technology can offer a variety of services, including 'peer-to-peer services'—services that are isolated from the traditional PSTN. These allow users to make and receive calls only over the internet.[160] Alternatively, VoIP technology can offer 'any-to-any connectivity' services, allowing users to make and receive calls to and from any telephone number.[161]

6.80 VoIP services will usually be classified as carriage services for the purposes of the *Telecommunications Act 1997* (Cth).[162] This means that VoIP service providers will generally be 'carriage service providers' that are required to observe the provisions in Part 13 of the *Telecommunications Act 1997* that protect the confidentiality of telecommunications information. These provisions are discussed in Part J. If, however, a VoIP service does not connect with the PSTN at all, the service provider may not be

156 Ibid, Rec 8–4.
157 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 30 July 2007.
158 For example, Skype software enables users to access VoIP services.
159 Australian Government Department of Communications Information Technology and the Arts, *Examination of Policy and Regulation Relating to Voice Over Internet Protocol (VOIP) Services* (2005), 14.
160 Ibid, 14–15.
161 Ibid, 15.
162 Ibid, 19.

regulated by the *Telecommunications Act 1997* but may be regulated by the *Privacy Act.*[163]

6.81 A concern that has arisen in relation to VoIP technology is that Australians may access voice services from providers outside Australia.[164] This may impact on the standards of protection for personal information disclosed during a VoIP call.[165] The OPC Review recommended that the Australian Government initiate discussions in international forums to deal with international jurisdictional issues arising from the global reach of new technologies such as VoIP.[166] VoIP technology is discussed further in Part J.

Location detection technologies

6.82 A number of technologies can provide real time information about the location of devices, and hence the location of users of the devices. The types of devices that can be located include mobile telephones, laptop computers, personal digital assistants and gaming consoles.[167] Location detection technologies, such as the global positioning system (GPS), are included as a standard feature in many 'next generation' mobile phones.

6.83 The accuracy of location information varies depending on the location detection technology used. For example, GPS can be used to determine the location of a device with a high degree of accuracy if the device transmits its position. The GPS is a network of 24 satellites established and operated by the United States Department of Defense.[168] Each satellite emits a signal that can be detected by a receiver. The satellites are positioned so that a minimum of four can be simultaneously detected by a receiver anywhere on the Earth's surface.[169] A receiver can determine its location with a high degree of accuracy by calculating the amount of time it takes for the signals emitted by the satellites to reach it.[170] Alternatively, the location of a mobile telephone can be determined with a moderate degree of accuracy by calculating the time a signal takes to receive three or more base stations.[171] Geo-location technologies can determine the location of an individual's IP address with a degree of accuracy that,

---

163 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 26.
164 Ibid, 25.
165 Ibid, 25.
166 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 70.
167 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.
168 Australian Communications Authority, *Location Location Location* (2004), 32.
169 Ibid, 32.
170 Ibid, 33.
171 Ibid, 31, 34.

depending on source and circumvention factors, ranges from country to city, to street level.[172]

6.84 Location detection technologies and other wireless technologies allow 'location-based services' to be provided to individuals.[173] There are many types of location-based services, including services that assist individuals to travel to particular locations; inform individuals about local conditions, such as traffic and weather conditions; provide individuals with information about goods or services in their immediate vicinity, and target advertising of goods and services to individuals on the basis of their location.[174]

6.85 Location detection technologies may also enhance service delivery by emergency services. Emergency call persons in Australia utilise subscriber information in the Integrated Public Number Database to determine the location of users of fixed telephone lines.[175] They are unable, however, to determine accurately the location of users of mobile telephones.[176] In the United States, mobile telephone providers are required to provide emergency call persons with precise information about the location of the mobile telephone used to call the emergency service.[177]

6.86 Location detection services enable the location of individuals to be determined in real time. Further, they generate records of the physical movements of individuals. For this reason, they have the potential to impact significantly on privacy. By analysing information about the location of an individual, a third party may derive or infer personal information about an individual, such as information about his or her consumer preferences or social activities.

6.87 The European Union Directive on privacy and electronic communications deals explicitly with 'location data' in the electronic communications sector.[178] Location data is defined as 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.[179] The Directive prohibits the processing of location data that has not been anonymised without the consent of the user of the service.[180] It also requires service providers to inform users, before obtaining their

---

172 D Svantesson, *Geo-identification—Now They Know Where You Live* (2004) Bond University Faculty of Law, 2.

173 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.

174 See, eg, Ibid, 4; M James, *Where are You Now? Location Detection Systems and Personal Privacy* (2004) Parliamentary Library—Parliament of Australia.

175 Australian Communications Authority, *Location Location Location* (2004), 17. The Integrated Public Number Database is discussed in Part J.

176 Ibid, 18.

177 See Federal Communications Commission, *Enhanced 911—Wireless Services* (2006) <www.fcc.gov/911/enhanced911> at 30 July 2007.

178 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).

179 Ibid, art 2.

180 Ibid, art 9(1).

consent, of the type of location data to be processed, the purpose and duration of the proposed processing, and whether the data will be transmitted to a third party for the purpose of providing a value added service.[181] Users must be given the opportunity to withdraw their consent at any time to the processing of location data.[182] Further, processing of the data must be restricted to that which is necessary for the purposes of providing the value added service.[183] Location detection technologies are discussed further in Part J.

Surveillance technologies

6.88 Surveillance involves the monitoring of a person, place or object to obtain certain information or to alter or control the behaviour of the subject of the surveillance.[184] Surveillance can be covert or overt and can be conducted by a variety of individuals, agencies or organisations for different reasons. For example, surveillance can be conducted by authorities to prevent or investigate crime, by the media to obtain commercially valuable information, or by individuals to monitor the activities of family members. The practice of surveillance is antithetical to privacy because the goal of surveillance is to 'pierce the privacy shield'.[185] While surveillance is said to be 'at least as old as recorded history',[186] developments in surveillance technology and the increased availability of this technology pose significant risks to privacy.

6.89 In ALRC 22, the ALRC considered the use of listening devices. It concluded that, as a general principle, an individual's private communications should not be monitored without his or her consent.[187] Accordingly, it recommended that legislation prohibit the use of listening devices for non-consensual or secret surveillance,[188] with some exceptions for the use of listening devices for law enforcement purposes and for 'participant monitoring'.[189]

6.90 In ALRC 22 the use of optical surveillance devices was also considered. The ALRC noted that the 'growth and increased sophistication of modern technological surveillance devices make it imperative that some legislative control be imposed on

181 Ibid, art 9(1).
182 Ibid, art 9(1), (2).
183 Ibid, art 9(3).
184 R Clarke, *Have We Learnt to Love Big Brother?* (2005) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html> at 30 July 2007.
185 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001), [1.5].
186 Ibid, [1.18].
187 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1122].
188 Ibid, Recs 28, 30.
189 Ibid, Recs 29, 40–50. Participant monitoring can occur: when a party to a private conversation uses a listening device to record the conversation without the consent of the other party; and when a party to a private conversation uses a listening device to transmit the conversation to someone who is not a party. Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1127].

their use for optical surveillance'.[190] The ALRC concluded that there should be no regulation of optical surveillance in public places—where individuals could expect to be observed—but recommended that the use of optical surveillance devices to observe people who would otherwise reasonably expect to be safe from observation be prohibited.[191] The ALRC recommended that there should be exceptions to the general prohibition on optical surveillance in private places, such as an exception for the use of an optical surveillance device by a person for the purpose of observing what, on reasonable grounds, appeared to be the commission of an offence, and an exception for the use of an optical surveillance device for law enforcement purposes.[192]

6.91 There are infinite innovations in the design of surveillance technologies. Currently, surveillance devices are used by agencies and organisations for a variety of purposes, including to prevent criminal activity and to monitor access to property. Some surveillance technologies, such as Closed Circuit Television (CCTV), can be combined with software that operates automatically to detect certain matters of interest.[193] For example, CCTV surveillance systems can be used in combination with character recognition technologies to enable automatic number plate recognition. Automatic number plate recognition systems extract the text of number plates from visual images of cars for a number of purposes, such as to compare them to records of stolen vehicles and unregistered cars.[194] Intelligent software can reduce the need for live monitoring of surveillance systems and reduce costs associated with recording irrelevant activity.[195]

6.92 The use of surveillance devices by federal law enforcement officers is regulated by the *Surveillance Devices Act 2004* (Cth). A surveillance device is defined as 'a data surveillance device, a listening device, an optical surveillance device or a tracking device', a device that is a combination of any two or more of these types of devices, or a device prescribed by regulations.[196] Generally, federal law enforcement officers must obtain a warrant to use a surveillance device. In certain circumstances, however, a surveillance device can be used without a warrant if use of the device does not involve entry onto premises, or interference with any vehicle or thing, without permission.[197] In addition, a listening device can be used without a warrant if an officer is participating in the conversation.[198] The use of surveillance devices by the Australian Security Intelligence Organisation is regulated by the *Australian Security Intelligence Organisation Act 1979* (Cth), while the intelligence gathering functions of the Australian Security Intelligence Service and the Defence Signals Directorate are set out in the *Intelligence Services Act 2001* (Cth).

---

190 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1187].
191 Ibid, Recs 52–53.
192 Ibid, Recs 53–54.
193 Council of Australian Governments, *A National Approach to Closed Circuit Television* (2006), 18.
194 See, eg, T Holding (Victorian Minister for Police and Emergency Services), 'Government to Keep Eye on Number Plate Trial' (Press Release, 16 March 2005).
195 Council of Australian Governments, *A National Approach to Closed Circuit Television* (2006), 18.
196 *Surveillance Devices Act 2004* (Cth) s 6(1).
197 Ibid ss 37–39.
198 Ibid s 38.

6.93 The handling of personal information obtained by the use of surveillance devices is generally regulated by the *Privacy Act* when the use of the device involves the collection of personal information for inclusion in a record. As noted in Chapter 1, the Victorian Law Reform Commission is currently examining surveillance in public places as part of a larger inquiry into privacy. It is anticipated that the recommendations resulting from this Inquiry will be considered by the Standing Committee of Attorneys-General.

Other developing technologies

6.94 There are other developing technologies that have the potential to impact adversely on privacy. For example, it has been argued that electronic number mapping (ENUM) may provide agencies, organisations and individuals with increased ability to track others.[199] ENUM is 'an electronic numbering system that can link the public telephone network and the internet by allowing telephone numbers to be converted into internet domain names'.[200] In summary, ENUM enables telephones connected to the internet to make calls to the Public Switched Telephone Network (PSTN) and receive calls from the PSTN.[201] The Australian Communications and Media Authority submitted that the next development in ENUM technology, infrastructure ENUM, will involve the mapping of blocks of ENUM registrations 'to a single Internet resource—generally a Voice over Internet Protocol (VoIP) address'.[202] One application of infrastructure ENUM could involve the 'peering'—or direct connection—of VoIP services in isolation from the PSTN.[203]

6.95 Digital Rights Management (DRM) technologies also have the potential to impact adversely on privacy. DRM technologies enable copyright owners to protect digital material by controlling the ways in which the material is accessed, used, copied and distributed.[204] It has been noted that virtually all DRM technologies require the collection of personal information about consumers of copyright material.[205] Accordingly, they limit the ability of these consumers to access material anonymously.

6.96 Further, DRM technologies can be used to monitor the activities of consumers by collecting information about the 'content used, the time of use, the frequency of use,

---

199 R Clarke, 'ENUM—A Case Study in Social Irresponsibility' (2003) 9 *Privacy Law & Policy Reporter* 181, 181.

200 Australian Communications Authority, *Annual Report 2004–05* (2005), 36.

201 Australian Communications and Media Authority, *What is ENUM or Electronic Number Mapping?* <www.acma.gov.au> at 30 July 2007.

202 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

203 See, eg, Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 July 2007.

204 Information and Privacy Commissioner Ontario, *Privacy and Digital Rights Management (DRM): An Oxymoron?* (2002), 2.

205 Ibid, 4.

and the location of use'.[206] The Australia-United States Free Trade Agreement requires the parties to introduce a scheme imposing liability for activites relating to the circumvention of 'effective technological measures' used by copyright owners to protect their material.[207] In September 2006, the Attorney-General of Australia released an exposure draft of amendments to the *Copyright Act 1968* (Cth) and the *Copyright Regulations 1969* (Cth) intended to implement this requirement of the Australia-United States Free Trade Agreement.[208]

6.97 Another area of concern relates to the use of application service providers. An application service provider is a business that enables customers to access software applications over a network, typically the internet. Use of an application service provider may result in large amounts of a customer's data being stored remotely.[209] The ALRC is interested in hearing about other technologies that may impact on privacy. The next chapter considers how best to accommodate these techologies in a regulatory framework.

206 D Mulligan, J Han and A Burstein, 'How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use"' (Paper presented at Proceedings of the 3rd ACM Workshop on Digital Rights Management, Washington DC, 27 October 2003).

207 *Australia-US Free Trade Agreement*, 18 May 2004, [2005] ATS 1, (entered into force generally on 1 January 2005), art 17.4.7.

208 Australian Government Attorney-General's Department, *Exposure Drafts—Copyright Amendment (Technological Protection Measures) Bill 2006 and related Regulations* <www.ag.gov.au> at 30 July 2007.

209 See, too, the discussion of transborder data flows in Ch 28.

Part B

Developing Technology

7. Accommodating Developing Technology in a Regulatory Framework

Contents

Introduction 341
Should the *Privacy Act* be technologically neutral? 342
Submissions and consultations 342
ALRC's view 344
Designing a 'technologically aware' framework 346
Privacy enhancing technologies 347
Empowering the individual 348
Statutory protection 350
The proposed Unified Privacy Principles 350
Definitions in the *Privacy Act* 352
Standards 354
Standards Australia 355
Standards bodies in other jurisdictions 355
Mandating standards 356
The role of the regulator 358
Proactive regulation 358
Oversight functions of the OPC 359
Research and monitoring 359
Education 360
Guidance on particular technologies 361
Background 361
Setting out requirements in the proposed UPPs 362
Automated decision review mechanisms 365
Data-matching 367
Co-regulation 372
Internet Industry Association Draft Code 373
Biometrics Institute Code 373
Other regulatory mechanisms 374

Introduction

7.1 This chapter discusses how to accommodate developing technology in a regulatory framework. The chapter first considers whether the *Privacy Act 1988* (Cth) should attempt to regulate the handling of information by specific technologies or whether the *Privacy Act* should be technologically neutral. The remainder of the

chapter discusses mechanisms that ensure that a technologically neutral *Privacy Act* remains technologically *aware*. The chapter considers the interaction between privacy enhancing technologies (PETs) and the individual. The chapter then summarises the proposed amendments to the *Privacy Act* that are relevant to technology, and proposes a proactive mechanism to mandate privacy and security standards in the *Privacy Act*. Finally, the chapter discusses the important role of the Office of the Privacy Commissioner (OPC) in protecting individual privacy in light of technological developments.

Should the *Privacy Act* be technologically neutral?

7.2 The explanatory memorandum to the Privacy Amendment (Private Sector) Bill 2000 noted that the National Privacy Principles (NPPs) were intended to be technologically neutral. Technologically neutral privacy principles were intended to ensure that the *Privacy Act* remained flexible and relevant in the case of technological change.[1] In Chapter 6, the ALRC considers the impact on privacy of several new and developing technologies. These technologies facilitate easier, cheaper and faster methods by which information may be collected, accessed, aggregated and communicated. Further, there is an increasing ability to store large quantities of information. In light of these technological developments—many of which have increased in application since 2000—the ALRC asked in Issues Paper 31, *Review of Privacy* (IP 31) whether technological neutrality should remain the objective of the *Privacy Act*.[2]

Submissions and consultations

7.3 The overwhelming majority of stakeholders who commented on this issue indicated that the *Privacy Act* should remain technologically neutral.[3] This view was based on several considerations. First, technology is developing at such a rate that attempts to regulate certain technologies through the *Privacy Act* will quickly render the legislation out-of-date. The Victorian Society for Computers and the Law noted that this is also the case for 'classes of technologies, given that these may change or merge over time'.[4] It was also noted in submissions that the impact on privacy of future applications of existing technologies may be difficult to predict.[5]

---

1 Further Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 9.

2 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 11–4.

3 See, eg, Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; M Fenotti, *Submission PR 86,* 15 January 2007; Australia Post, *Submission PR 78,* 10 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

4 See, eg, Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.

5 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

7.4 The Australian Retailers Association submitted that reference to specific technologies in the *Privacy Act* may, by implication, exclude from its ambit other technologies that have a significant impact on privacy.[6]

7.5 Microsoft Australia noted that the international 'patchwork' of privacy legislation resulted in commercial challenges. In supporting technologically neutral legislation generally, Microsoft noted that nationally legislated privacy protection may operate as a 'tariff' on transborder flows of information. Microsoft submitted that technologically neutral privacy principles interacted well with 'international privacy frameworks and domestic privacy law in other countries'.[7]

7.6 The Australian Communications and Media Authority suggested that responding to the impact of developing technology on privacy could be informed less by reference to technology and more by the 'two more stable considerations' of consumer privacy expectations and the 'conduct of organisations in using personal and sensitive information'.[8]

7.7 The OPC suggested that an effective approach to regulating technology would involve some amendment to a technologically neutral *Privacy Act* to ensure that the Act remains both 'technologically neutral' and 'technologically relevant'.[9]

7.8 Stakeholders in support of a technologically neutral *Privacy Act* suggested that the impact of technology on privacy could be addressed by technologically specific legislation, regulations, guidelines or binding codes. For example, the Australian Privacy Foundation submitted that privacy laws

> need to be as 'technology neutral' as possible so that the objective of the principles are satisfied irrespective of the medium or channel used. At the same time, some technologies are known to raise particular issues (such as VoIP, RFID and so-called geo-identification), and it may be appropriate to address these specifically as they arise, either by amendment of the law, or through Codes of Practice and Guidelines.[10]

7.9 The OPC submitted that:

> To accommodate particular technologies that create privacy risks which fall outside the scope of privacy legislation, the Privacy Act should provide for the Commissioner to make binding codes that go to certain acts or practices or certain technologies …

---

6 Australian Retailers Association, *Submission PR 131,* 18 January 2007.
7 Microsoft Australia, *Submission PR 113,* 15 January 2007
8 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007. A similar point was made by the Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.
9 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
10 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

> This would facilitate timely responses to new technologically specific privacy issues.[11]

Contrary views

7.10 Professor Roger Clarke queried whether the concept of technological neutrality operates effectively in practice.[12] For example, Clarke has noted previously that the impact of some technologies on privacy may be inconceivable until the technologies have actually been invented and deployed.[13] One submission queried the adequacy of a technologically neutral *Privacy Act* given 'the introduction of the SPAM Act which was in direct response to the abuse of a reasonably new technology by marketers'.[14]

7.11 In addition, the Legal Aid Commission of New South Wales noted that technologies such as optical surveillance devices can collect information not covered by the *Privacy Act.* For example, the privacy principles apply only to personal information collected for inclusion in a 'record'. The Legal Aid Commission submitted that the privacy principles may not be able to regulate adequately developing technologies.

> The [I]nformation Privacy Principles (IPPs) and National Privacy Principles (NPPs) are based on the way data was processed in the late 1970s, before the Internet, desktop computers, and widespread applications of digital sound and visual recording and telephony. They assume computer systems that were designed to process information in pre-defined ways, rather than contemporary customer relationship or client management systems that are designed to record a flexible range of interactions between organisations and people. They assume that information is disclosed by individuals at a definite point in time and can be regulated at distinct stages of collection, storage, use and disclosure and by establishing clear lines of custodial responsibility for the way personal information [is] handled.[15]

7.12 Finally, Professor William Caelli submitted that no law is truly 'technologically neutral', noting that it is unclear

> just what is meant by the term 'technology neutral' ... perhaps we mean that the Act should be 'artefact' neutral in that no specific manifestation of a given technology is specified.[16]

ALRC's view

7.13 Making the *Privacy Act* technologically (or artefact) neutral is the most effective way to ensure individual privacy protection in light of developing technology.[17] Current technologies do not alter fundamentally the nature of the information-handling

---

11 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
12 R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.
13 R Clarke, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 25 February 2005, 2.
14 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.
15 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
16 W Caelli, *Submission PR 99,* 15 January 2007.
17 While the ALRC accepts Professor Caelli's point, the ALRC has decided to use the term 'technologically neutral' as it is the more commonly understood term. Note, however, that a technologically neutral *Privacy Act* does not preclude the use of words such as 'technology'.

cycle. For example, surveillance devices and radio frequency identification (RFID) systems may facilitate the collection of personal information without the knowledge or consent of an individual but the *collection* of the information will still be regulated by the 'Collection' principle in the proposed Unified Privacy Principles (UPPs) set out in the beginning of this Discussion Paper. Similarly, personal information that is shared electronically will be regulated by the proposed 'Use and Disclosure' principle. In addition, storage and destruction of personal information that is held in an electronic form must take place in line with the requirements in the proposed 'Data Security' principle. The ALRC's view, therefore, is that the handling of personal information by developing technologies can be regulated by high level and technologically neutral UPPs.[18] It is not desirable to propose an entire overhaul of the *Privacy Act* on the basis that technologies, which are yet to be invented or deployed, may not be accommodated by the proposed UPPs.

7.14 The OPC has the function to research and monitor developments in technology and to report to the Minister the results of such research and monitoring.[19] The ALRC is of the view that the OPC could exercise this function to provide a continuing review mechanism of the adequacy and effectiveness of the *Privacy Act* in light of further developments in technology.

7.15 The enactment of separate legislation directed towards particular technologies does not of itself represent a failure of a technologically-neutral *Privacy Act*. Instead, it indicates that information handled by particular technologies may require stronger protection in certain, limited circumstances. In addition, while the *Privacy Act* should be technologically neutral, some technologies that impact on privacy may require regulation through standards and legislative instruments. This chapter discusses mechanisms to ensure that a technologically-neutral *Privacy Act* does not result in a technologically *blind* privacy framework.

7.16 Finally, a number of concerns raised by stakeholders in this Inquiry about the impact of technology on privacy are dealt with in other sections of this Discussion Paper. In Part A, the ALRC proposes amendments to the definitions of 'personal information', 'sensitive information' and 'record'. In Part D, the ALRC proposes several amendments to the privacy principles. In Part F, the ALRC proposes additional OPC powers and functions that are relevant to technological developments. These proposals are discussed below and in Chapter 8.

Proposal 7–1 The *Privacy Act* should be technologically neutral.

18 Proposal 15–1.
19 *Privacy Act 1988* (Cth) s 27(1)(c).

Designing a 'technologically aware' framework

7.17 The OPC submitted that the privacy regulatory framework should be informed by the assumption that 'information will be handled in electronic form'.[20] The OPC cited a University of California, Berkeley study that found that only 0.01% of all new information produced in 2002 was paper-based.[21] Effective privacy protection, therefore, requires the development of a 'technologically aware' framework. The remainder of this chapter considers how to ensure that a technologically neutral *Privacy Act* remains relevant in light of developments in technology.

7.18 Professor Lawrence Lessig has described four modes of regulation in cyberspace, noting that these modes are reflected in 'real space'. These modes—and examples of their application in cyberspace—are as follows:

- *law*, which may include prohibitions and sanctions for online defamation and copyright infringement;
- *social norms*, which may involve a user conforming the behaviour of their avatar to community expectations in an online world such as Second Life or a social networking site such as Facebook;
- *markets*, which regulate the price paid for access to the internet and access to information on the internet; and
- *architecture*, which is the code, hardware or software that shapes the appearance of cyberspace.[22]

7.19 Cyberspace regulatory theorists disagree on the role that should be taken by each modality in Lessig's analysis.[23] Lessig demonstrates, however, that regulation of the internet and other developing technologies must be through measures additional to conventional 'law'. Otherwise, the regulation through law can be circumvented or undermined by, for example, the architecture of the internet.

7.20 As a starting point, broadly drafted statutory principles could address developing technology. A regulatory framework, however, should also accommodate co-regulation between the OPC and agencies and organisations, and it should seek to empower individuals by providing them with mechanisms to protect their privacy. A focus on the deployment of PETs by agencies, organisations and individuals underpins the framework suggested in this chapter.

---

20 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

21 Ibid.

22 L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501, 507–510.

23 See, eg, D Post, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' (2000) 52 *Stanford Law Review* 1439.

7.21 A technologically aware regulator plays a crucial role in dealing with the impact of technology on privacy. In this chapter, the ALRC proposes that the OPC should provide guidance that outlines how certain requirements in the proposed UPPs can be met by agencies and organisations that use particular technologies to handle information.[24]

7.22 Education is a further important feature of the regulator's role. In this chapter, the ALRC proposes that the OPC should educate individuals about how to use PETs to protect their privacy. In addition, education programs focused on PETs should be directed towards agencies and organisations that design and deploy new and developing technologies.[25]

7.23 In Chapter 44, the ALRC discusses the importance of proactive regulation. This is reflected in the proposals to empower the OPC to conduct audits of records held by both agencies and organisations, and direct privacy impact assessments for new projects and developments.[26] These proposals are intended, in part, to promote the early implementation of PETs.

7.24 Finally, while this chapter focuses on domestic regulation of developing technology, the global nature of technology development and deployment requires industry, the OPC, and the Australian Government to coordinate and engage with others in the international arena. The OPC noted its support for 'Australia's involvement in international forums to coordinate data protection schemes'.[27] A report prepared by the Australian Communications Authority in 2005 made a similar point.[28]

Privacy enhancing technologies

7.25 A number of stakeholders submitted that the Inquiry consider the role that PETs could play in a regulatory framework.[29] The term 'PETs' can be used in a number of different contexts. PETs can refer to particular technologies that form part of the architecture of technological systems used by agencies and organisations to deliver services.[30] Chapter 6 includes a discussion of these types of PETs, which may include mandatory access control devices or identity management systems. Secondly,

---

24 Proposal 7–5.
25 Proposal 7–4.
26 See Proposals 44–4 and 44–6.
27 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
28 Australian Communications Authority, *Vision 20/20: Future Scenarios for the Communications Industry—Implications for Regulation* (2005), 37.
29 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; Australian Electrical and Electronic Manufacturers' Association, *Submission PR 124,* 15 January 2007 Edentiti, *Submission PR 29,* 3 June 2006.
30 Commission of the European Communities, *Communication From the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 (2007), 3.

individuals can utilise PETs to exercise control over the collection of their personal information.[31] Chapter 6 discusses several of these types of PETs, including encryption and RFID signal 'blockers'. Finally, the way that technology is used often determines whether its impact is privacy enhancing or invasive.[32] An holistic approach to regulating technology would encourage agencies and organisations to develop and deploy all technologies to enhance privacy.

7.26 In May 2007, the European Commission issued a communication on PETs to the European Parliament and Council, noting that PETs were most effective when 'applied according to a regulatory framework of enforceable data protection rules'.[33] The ALRC's view is that PETs promote enhanced security and trust and are therefore an essential component of the regulatory structure. Some PETs, however, can be physically unwieldy and costly to implement. Moreover, use of PETs may require a certain level of technological expertise. PETs alone, therefore, cannot address the impact of technology on privacy and should complement, rather than replace, the legislative and regulatory structure outlined below.

Empowering the individual

7.27 Use of PETs by individuals—and education of individuals about PETs—can provide individuals with greater control over their personal information when using technologies such as the internet. The OPC submitted that:

> Education and PET solutions together will be crucial for dealing with the international nature of the internet and for ensuring that individuals are able to exercise appropriate control of their personal information when its handling falls outside of the national jurisdiction of Australian privacy law.[34]

7.28 A national survey conducted in May 2007 found that Australians were more concerned about online privacy than the threat of a terrorist attack.[35] PETs, therefore, could play a role in increasing consumer trust in online interactions. Chapter 6 discusses two main types of PETs that may be deployed by individuals to protect their privacy online: encryption and identity management.

7.29 In Chapter 5, the ALRC proposes that the *Privacy Act* be amended to include a statutory cause of action for invasion of privacy.[36] The proposed statutory cause of action may be commenced against an individual acting in a non-commercial capacity—such as an internet blogger who does not fall within the definition of a 'media organisation'—as well as against an agency or organisation. In addition to

---

31 Ibid, 3–4.

32 See, eg, J Alhadeff, *Consultation*, Sydney, 26 April 2007; M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002), 9–10.

33 Commission of the European Communities, *Communication From the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 (2007), 4.

34 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

35 Unisys, *Unisys Security Index Australia: A Newspoll Survey May 2007*, 1 May 2007.

36 Proposal 5–1.

using PETs, therefore, individuals may be able to obtain, if the ALRC's proposal is implemented or the common law continues to develop, remedies for invasion of privacy.

7.30 Some commentators have also suggested that individuals could benefit from the introduction of property or market-based schemes.[37] Such schemes are based on the premise that individuals should have the right of ownership over their personal information and, therefore, enjoy commercial exploitation of this information. It has been noted, however, that property and market-based rights schemes have a number of drawbacks. For example, it has been questioned whether personal information is ever freely alienable.[38] It has also been argued that the 'market approach has difficulty assigning the proper value to personal information'.[39]

7.31 In the ALRC's view, promoting mechanisms that enhance individual control over personal information is one way to deal with the protection of individual privacy in light of technological developments. Emphasising only the responsibility of individuals to protect their information privacy is undesirable. It places a 'premium' on the individual

> having sufficient interest in protection and the 'cultural capital'—the ability and the means to comprehend what is happening … to read obscure fine print on the web, and to assert herself in controlling inroads or seeking redress once these threats have been realised.[40]

7.32 Submissions made to the current review into the Electronic Funds Transfer (EFT) Code of Conduct, which is being conducted by the Australian Securities and Investments Commission (ASIC), should be considered in light of the reasonable limits of individual responsibility. For example, some banking and financial industry stakeholders submitted to ASIC that individuals who do not maintain a certain level of equipment security should be made liable under the EFT Code of Conduct 'for the full amount of losses from malicious code compromises of account access data'.[41] In the ALRC's view, shifting privacy risk from organisations to individuals using existing and developing technology is questionable from a policy perspective. The following sections consider the role of legislation and the OPC in regulating the impact of developing technology on privacy.

---

37 See, eg, J Rule, 'Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions' (2004) 54 *University of Toronto Law Journal* 183.

38 P Samuelson, 'Privacy as Intellectual Property?' (2000) 52 *Stanford Law Review* 1125, 1137–1147.

39 D Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 *Stanford Law Review* 1393.

40 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, 84.

41 Australian Securities and Investment Commission, *Reviewing the EFT Code—Consultation Paper 78* (2007), 64–66.

Statutory protection

7.33 This section focuses on the amendments to the *Privacy Act* that the ALRC proposes to ensure that the Act remains relevant in light of technological development. The section first discusses amendments to the proposed UPPs that are relevant to technology. The section then discusses proposed amendments to relevant definitions in the *Privacy Act*. Finally, the chapter proposes a mechanism for mandating appropriate privacy and security standards.

7.34 It should also be noted that, in some circumstances, regulation of specific technologies may be appropriate. The *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) are examples.[42] In the United States, several technologically specific bills are currently before Congress.[43]

The proposed Unified Privacy Principles

7.35 The proposed UPPs are intended to regulate personal information throughout the information-handling cycle. In formulating the UPPs, the ALRC addressed developments in technology by proposing several additions and amendments to the NPPs. Part D contains a detailed examination of each proposed UPP.

Anonymity and Pseudonymity

7.36 As discussed in Chapter 17, a number of stakeholders submitted that the 'Anonymity' principle in the NPPs should be expanded to deal with pseudonymous interactions. Having the option to transact anonymously provides an individual with control over what information is collected about them by an agency or organisation, particularly in an electronic environment. It may not always be practicable, however, for an agency or organisation to transact anonymously with individuals. In these circumstances it may be practicable for an individual with an authenticated identity to transact with an agency or organisation using a pseudonym.

7.37 The ALRC proposes that the privacy principle dealing with anonymity should also include a pseudonymity requirement that states that when an individual is transacting with an agency or organisation, the agency or organisation must give the individual the clear option of identifying themselves by a pseudonym. This requirement is limited to circumstances where providing this option is lawful, practicable and not misleading.[44] The ALRC also proposes that the meaning of the terms in this principle should be accompanied by guidance issued by the OPC.[45]

---

42 The ALRC discusses the regulation of specific telecommunications technologies in Part J.

43 See, eg, S 1625—Proposed Counter Spy Act of 2007 (US); HR 964—Proposed Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) of 2007 (US); HR 1525—Proposed Internet Spyware (I-SPY) Protection Act of 2007 (US).

44 Proposal 17–2.

45 Proposal 17–4.

7.38 The proposed 'Anonymity and Pseuonymity' principle is the first listed principle in the proposed UPPs. It reflects

> the idea that the lifecycle of information begins before collection, when organisations and agencies should consider the fundamental question of whether they need to collect personal information at all.[46]

Collection

7.39 In Chapter 18, the ALRC proposes that, where an agency or organisation receives unsolicited personal information, it must either: (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.[47] This proposal provides a mechanism for dealing with circumstances when an agency or organisation might inadvertently 'collect' information—for example, when information electronically 'passes over' a system.

7.40 The *Privacy Act* does not require agencies or organisations to obtain an individual's consent before collecting personal information. On the other hand, sensitive information is subject to greater restrictions and, usually, consent is required in order to collect sensitive information. In IP 31, the ALRC asked whether there are categories of personal information that can be collected by new technologies that should only be collected with consent.[48] Two stakeholders submitted that consent should be obtained prior to the collection of information by RFID or biometric systems.[49] Several stakeholders, however, opposed the introduction into the 'Collection' principle of a requirement that an agency or organisation needs to obtain consent prior to the collection of personal information by certain technologies because such a requirement would be inconsistent with the technological neutrality of the *Privacy Act*.[50]

7.41 The OPC submitted that another approach may be to 'increase protections for particular types of information rather than particular types of technology'.[51] The ALRC agrees with this approach. In Chapter 3, the ALRC proposes that biometric

---

46 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
47 Proposal 18–2.
48 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.126].
49 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; Health Informatics Society of Australia, *Submission PR 196,* 16 January 2007.
50 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.
51 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

information, collected for certain purposes, should be included in the definition of sensitive information.[52]

Specific notification

7.42 As discussed in Chapter 6, technologies such as optical surveillance devices and computer software can allow the collection of information about an individual from that individual without his or her knowledge.

7.43 In Chapter 20, the ALRC proposes that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of, amongst other things, the fact and circumstances of collection (for example, how, when and from where the information was collected).[53] This will provide the individual with the knowledge that their information has been collected, and some understanding of how technology was used to collect it.

Identifiers

7.44 In Chapter 27, the ALRC notes that agencies increasingly use biometric information such as photographs as identifiers. The ALRC therefore proposes an amended definition of an 'identifier' in the proposed 'Identifiers' principle that makes it clear that the definition includes biometric information that is used as an identifier.[54]

Data breach notification

7.45 In IP 31, the ALRC asked whether there should be a new privacy principle dealing with data breach notification. The ALRC noted that breaches of data security are particularly relevant in the context of developing technology given that technologies such as the internet can provide a vehicle for the widespread dissemination of personal information.[55]

7.46 In Chapter 47, the ALRC proposes that the *Privacy Act* be amended to include a new Part on data breach notification. Generally, an agency or organisation would be required to notify the Privacy Commissioner and affected individuals when a data breach occurs and unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.[56]

Definitions in the *Privacy Act*

7.47 This section outlines the amendments to definitions of terms in the *Privacy Act* that are relevant to technology. Detailed discussion of the following amendments is contained in Chapter 3.

---

52 Proposal 3–6.
53 Proposal 20–2.
54 Proposal 27–2.
55 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.140].
56 Proposal 47–1.

Personal information

7.48 In IP 31, the ALRC asked whether the definition of personal information was adequate and appropriate in light of advances in technology.[57] The ALRC noted that, in some circumstances, information such as an individual's Internet Protocol (IP) address, mobile telephone number, email address or biometric information will not be personal information because it does not enable the *identity* of an individual 'reasonably [to] be ascertained'.[58] In the context of RFID technology, it could be argued that information about tagged items in an individual's possession may not be personal information if the identity of the individual cannot 'reasonably be ascertained'. These types of information, however, may enable individuals to be contacted, tracked or profiled.

7.49 In 2000, the Senate Select Committee on Information Technologies recommended that the *Privacy Act* be amended to regulate the collection of personal information through the use of technologies such as cookies and web bugs, which could indirectly identify consumers.[59] It suggested that this could be achieved by amending the definition of 'personal information' in the Act.

7.50 In Chapter 3, the ALRC proposes that 'personal information' be defined in the *Privacy Act* as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.[60] This means that once information is able to be linked to an individual—and that individual is able to be contacted or targeted—it would become personal information for the purposes of the *Privacy Act.* The proposed definition would mean that telephone numbers, email addresses or IP addresses are personal information for the purposes of the *Privacy Act* once a sufficient amount of other information accretes around such points of contact.

Sensitive information

7.51 In IP 31, the ALRC asked whether the definition of sensitive information should include types of personal information collected by new technologies.[61] A number of stakeholders supported the amendment of the definition of 'sensitive information' to include biometric information. These submissions are discussed in Chapter 3. Limited feedback was received on other types of information that could be collected by existing and developing technologies.

7.52 The ALRC's view is that biometric information shares characteristics with other types of sensitive information and should be subject to more stringent protection than

---

57 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 3–4.
58 In terms of the definition of 'personal information' in *Privacy Act 1988* (Cth) s 6(1).
59 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), rec 4.
60 Proposal 3–5.
61 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.124].

non-sensitive personal information. Biometric information can be very difficult to replace once it has been accessed improperly. Further, biometric information may reveal health, genetic, racial and ethnic information about an individual. The ALRC notes, however, that it is neither necessary nor practicable to classify all types of biometric information as 'sensitive information'. In Chapter 3, the ALRC proposes that the definition of 'sensitive information' in the *Privacy Act* should be amended to include (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information.[62]

Record

7.53 It has also been noted that the requirement that personal information be held or collected for inclusion in a record means that some privacy invasive practices, such as the use of live closed circuit television (CCTV), are not governed by the *Privacy Act*.[63] It has been argued that consideration should be given to ensuring that agencies and organisations are not allowed to breach the spirit of the *Privacy Act* by avoiding making a record.[64] As noted in Chapter 1, the Victorian Law Reform Commission is currently examining surveillance in public places as part of a larger inquiry into privacy. It is anticipated that the recommendations resulting from that inquiry will be considered by the Standing Committee of Attorneys-General.

7.54 In Chapter 3, the ALRC proposes that the definition of 'record' in the *Privacy Act* should be amended to include (a) a document; and (b) information stored in electronic or other form. The *Acts Interpretation Act 1901* (Cth) defines a document to include an image, which covers photographs and other pictorial representations.[65]

7.55 The ALRC notes that the definition of a record excludes a 'generally available publication'.[66] This means that several of the proposed UPPs do not apply to personal information in generally available publications. Publicly available information, including the concept of a generally available publication, is examined further in Chapter 8.

Standards

7.56 Another way to minimise the impact of developing technology on privacy is to require software and hardware systems to comply with certain technical standards before being released to the public or otherwise used. The term 'standardisation' can be used to refer to consistency and interoperability between technical systems. Standards

---

62 Proposal 3–6.

63 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19].

64 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [60]; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000, 7.

65 Proposal 3–8.

66 *Privacy Act 1988* (Cth) s 6(1).

also require compliance with certain specifications and procedures that are intended to result in appropriate levels of safety, privacy or security.

7.57 It has been noted that information security is increasingly relevant to privacy.[67] Local and international bodies are continuing to develop standards on privacy and security issues such as identification, authentication and encryption. This section examines several privacy and security standards that could be applied in Australia.

Standards Australia

7.58 Standards Australia is the peak standards-developing body in Australia.[68] In the communications, information technology and e-commerce area, a number of privacy and security standards have been or are being developed, including in the areas of biometrics and identification and automatic identification and data capture techniques.[69] These standards are developed with the input of technical committees, which include industry, government and consumer stakeholders. Standards Australia also adopts several standards that are developed by international standards bodies such as the European Committee for Standardization, the International Standards Organization (ISO) and the International Electrotechnical Commission.[70]

Standards bodies in other jurisdictions

United States

7.59 The activities of the National Institute of Standards and Technology (NIST) include the development of standards and guidelines on information and communications technologies. NIST has published standards and guidelines on computer security, biometrics and digital information access. A number of other standards are being developed, including those on smart card security, anti-spam technologies, mobile and wireless security, personal identity verification and encryption.[71]

International standards

7.60 A number of international bodies have developed relevant privacy and security standards. The United Nations agency for information and communications technologies, the International Telecommunication Union (ITU-T), publishes privacy and security standards on RFID, biometric authentication, password-authenticated key

---

67 P Cullen, T Hughes and M Crompton, *Consultation PC 19*, Sydney, 8 May 2006.

68 Standards Australia, *Annual Report 2005–2006* (2006), 1.

69 Standards Australia, *Communications, IT & e-Commerce* <www.standards.org.au/cat.asp?catid=37> at 16 July 2007.

70 Standards Australia, *Annual Report 2005–2006* (2006), 9.

71 See, eg, National Institute of Standards and Technology, *Technology Services: Standards and Technical Regulations* <ts.nist.gov/Standards/ssd.cfm> at 16 July 2007.

exchange, spyware and anonymous authentication architecture systems.[72] The ISO, which comprises 157 national standards bodies, is developing privacy standards on biometric systems and has published standards on the security of information processing systems, identification cards and banking and personal identification number management systems.[73]

7.61 The World Wide Web Consortium (W3C) develops open standards that aim to achieve trust and interoperability on the internet. These standards are developed by a W3C expert technical team with input from the public and W3C members. Membership of the W3C includes vendors of technology products and services, content providers, corporate users, research laboratories, standards bodies and governments.[74] The W3C Platform for Privacy Preferences (P3P) Working Group had developed a number of internet privacy specifications until work on this project was suspended at the end of 2006.[75]

7.62 The Common Criteria for Information Technology Security Evaluation (Common Criteria) is a standard that provides methods for evaluating the capabilities of various security products and techniques and establishing trust in these products and techniques.[76] In Australia, the Common Criteria is administered by the Defence Signals Directorate.[77]

7.63 Finally, the Payment Card Industry (PCI) Security Standards Council comprises a membership of five major credit card companies, including American Express and Visa. The PCI Security Standards Council has developed a data security standard that requires companies that handle customer information using the payment card services of its member organisations to comply with certain security policies and procedures for network architecture and software design.[78]

Mandating standards

7.64 Standards and codes developed by standards and industry bodies, as discussed above, can be a form of proactive privacy protection in a 'light-touch' regulatory regime. It has been noted, however, that there may not be adequate incentive for agencies and organisations to comply with standards because of a lack of adequate

---

72 See, eg, International Telecommunication Union, *Telecommunication Standardization Sector (ITU-T)* <www.itu.int/ITU-T/index.html> at 17 July 2007.

73 See, eg, International Organization for Standardization, *Standards Development* <www.iso.org/iso/en/stdsdevelopment/whowhenhow/how.html> at 17 July 2007.

74 See, eg, World Wide Web Consortium (W3C), *About the World Wide Web Consortium* <www.w3.org/Consortium/> at 17 July 2007.

75 World Wide Web Consortium (W3C), *Platform for Privacy Preferences (P3P) Project* <www.w3.org/P3P/> at 16 July 2007.

76 See, eg, Common Criteria, *The Common Criteria Portal* (2006) <www.commoncriteriaportal.org/index.php> at 16 July 2007.

77 See, eg, Australian Government Defence Signals Directorate, *Mutual Recognition and the Common Criteria Recognition Arrangement (CCRA)* <www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep_partners.html> at 16 July 2007.

78 See, eg, PCI Security Standards Council, *About the PCI Data Security Standard (PCI DSS)* <https://www.pcisecuritystandards.org/tech/index.htm> at 16 July 2007.

enforcement mechanisms. For example, it was noted recently that 83% of large merchants using Visa are not in compliance with the PCI Data Security Standard.[79] In addition, a proliferation of local and international standards for technologies such as voice over internet protocol (VoIP) and RFID can result in inconsistent privacy and security protection for individuals.[80]

7.65 Providing a mechanism for the introduction of appropriate privacy and security standards into legislation, therefore, would promote consistency in standards and compliance with such standards. Such a mechanism would ensure that security mechanisms and PETs are incorporated at the systems design stage.

Options for mandating standards

7.66 Standards Australia states on its website that 'around a third of all Australian Standards form some part of Territory, State or Federal law'.[81] An example of Australian legislation that incorporates standards is the *Motor Vehicle Standards Act 1989* (Cth). This Act provides for the making of legislative instruments that determine standards for road vehicles or vehicle components.[82] In determining these standards, the Minister may consult with relevant state or territory authorities, persons or organisations involved in the road vehicle industry, or organisations that represent road vehicle users.[83] The Act also provides for the incorporation of standards developed by national and international bodies.[84]

7.67 Other than in certain circumstances, the Act prevents the supply to the market of vehicles that do not comply with standards.[85] Further, a corporation that manufactures a vehicle that does not comply with the standard generally cannot use this vehicle for transport in Australia.[86]

ALRC's view

7.68 The *Privacy Act* should be amended to empower the Minister responsible for the *Privacy Act* (currently the Attorney-General)[87] to determine privacy and security standards for relevant technologies. This is a proactive approach that will ensure that appropriate privacy and security requirements form part of technical systems used by agencies, organisations and individuals. Providing the Minister with the power to

---

79 D Rosenblum, 'Achieving PCI Compliance with Storage Security Systems' (2007) (1) *Computer Technology Review* <www.wwpi.com>.

80 W Caelli, *Correspondence*, 2 April 2007.

81 Standards Australia, *What is a Standard?* <www.standards.org.au/cat.asp?catid=2> at 16 July 2007.

82 *Motor Vehicle Standards Act 1989* (Cth) s 7.

83 Ibid s 8.

84 Ibid s 7A.

85 Ibid ss 10A(2), 14.

86 Ibid s 15.

87 Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

determine relevant standards would not require the mandating of all privacy and security standards. Rather, it would allow the Minister to mandate certain standards where appropriate. This proposal strikes an appropriate balance in a light-touch regulatory regime.

7.69 The *Motor Vehicle Standards Act* is an instructive example in determining how to mandate appropriate privacy and security standards. In particular, the ALRC notes that s 7A provides for the mandating of relevant standards that have been developed by Australian and international standards bodies such as those outlined above.

7.70 The ALRC notes that the OPC has several functions and powers relevant to technology. For example, the OPC's research and monitoring function is intended to ensure that the OPC stays abreast of the impact of technology on privacy. The Minister should, therefore, determine relevant privacy and security standards in consultation with the OPC.

Proposal 7–2 The *Privacy Act* should be amended to empower the Minister responsible for the *Privacy Act*, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.

The role of the regulator

7.71 This part of the chapter considers the role of the OPC in dealing with the impact of developing technology on privacy.[88] The following section highlights the importance of proactive regulation in the face of developing technology. The chapter then discusses the OPC's oversight functions that relate to technology and the OPC's power to issue non-binding guidance for certain technologies. The chapter proposes instances where such guidance would be appropriate. Finally, the section considers the co-regulatory basis of the proposed enhanced power of the OPC to approve and direct the making of binding privacy codes in relation to certain technologies.

Proactive regulation

7.72 In Chapter 44, the ALRC discusses the desirability of early regulatory intervention in order to prevent interferences with privacy. Reflecting the emphasis that should be placed on proactive regulatory measures, the ALRC proposes that the *Privacy Act* be amended to empower the Privacy Commissioner to conduct audits of the records of organisations for the purpose of ascertaining whether an organisation's records are maintained according to the requirements in the proposed UPPs, privacy regulations and any privacy code that binds the organisation.[89] Further, the ALRC

88 See Ch 44 for a detailed discussion of the existing and proposed powers and functions of the OPC.
89 Proposal 44–6.

proposes that the OPC should have the power to direct agencies and organisations to conduct privacy impact assessments (PIAs) for new projects and developments.[90]

7.73 Audits and PIAs could be used to encourage compliance with requirements of the proposed UPPs to prevent a developing technology from having an adverse impact on privacy. For example, the proposed 'Anonymity and Pseudonymity' principle requires agencies and organisation to design systems that allow for anonymous or pseudonymous transactions where it would be 'practicable' to do so.[91] It has been noted that it may not be 'practicable' to alter retrospectively to alter systems such as biometric identification systems or transport systems using smart card technology to allow for anonymity in transactions.[92] PIAs, however, could ensure that agencies and organisations take privacy into account before the system is developed and develop and use systems that provide for anonymous or pseudonymous transactions.

Oversight functions of the OPC

Research and monitoring

7.74 The OPC has two research and monitoring functions that are relevant to the regulation of new and developing technologies. These are to:

- conduct research and monitoring into data processing and computer technology (including data-matching and data-linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;[93] and

- monitor and report on the adequacy of equipment and user safeguards.[94]

7.75 In Chapter 44, the ALRC proposes that the first function be amended to remove the word 'computer' to make it clear that the OPC's research and monitoring function is not limited to computer technology.[95]

7.76 In 2006, the UK Information Commissioner published a report noting that an effective regulator needs to stay 'abreast of, and knowledgeable about, new

90 Proposal 44–4.
91 See the proposed 'Anonymity and Pseudonymity' principle set out at the beginning of this Discussion Paper.
92 M Crompton, 'Biometrics and Privacy: The End of the World as We Know it or the White Knight of Privacy?' (Paper presented at Biometrics Institute Conference: Biometrics—Security and Authentication, Sydney, 20 March 2002).
93 *Privacy Act 1988* (Cth) s 27(1)(c).
94 Ibid s 27(1)(q).
95 Proposal 44–1.

technologies and systems'.[96] Noting the resource implications that this may involve, the report suggested that

> it is advantageous … to develop a pooled technological knowledge-and-awareness capability, as may be occurring, for instance, at the level of the EU, through the Article 29 Working Party and other networks and channels in which many national and sub-national regulators participate.[97]

7.77 The OPC's research and monitoring functions could be complemented by active engagement with international data protection networks. In Chapter 43, the ALRC proposes that the OPC be empowered to convene expert panels.[98] Such a panel could include experts in information and communication technologies.[99] Along with participation in international fora, advice from experts will equip the OPC with the relevant expertise to carry out its research and monitoring function and other powers and functions relevant to developing technology.

7.78 In the ALRC's view, the OPC should prioritise PETs when exercising its research and monitoring function. In particular, the function to research and monitor user safeguards could be used to research PETs such as online authentication and identity management systems.

Proposal 7–3 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations.

Education

7.79 The OPC also has the ability to undertake and coordinate educational programs for the purposes of promoting individual privacy.[100] The expertise attained by the OPC in exercising its researching and monitoring functions could form the basis of educational programs.

7.80 The OPC's education function is sufficiently broad to allow the OPC to conduct education programs that relate to the privacy impacts of technology on individuals.[101] In the ALRC's view, the OPC should conduct education programs which focus on specific PETs and the privacy enhancing ways in which technologies can be deployed. Such education programs should be directed towards those designing technical

---

96 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, 96.

97 Ibid, 96.

98 Proposal 43–5.

99 In addition, the OPC is required to include on its Advisory Committee a member with extensive experience in 'electronic data-processing': *Privacy Act 1988* (Cth) s 82(7)(c). In Ch 43, the ALRC proposes that the term 'electronic data-processing' in s 82(7)(c) be replaced with the term 'information and communication technologies': Proposal 43–4(c).

100 Ibid s 27(1)(m).

101 The OPC's education function is discussed further in Ch 44.

systems; agencies and organisations that use the systems to deliver services; and individuals that use such systems.

7.81 The ALRC also proposes that, to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy and, in particular, privacy in the online environment, into school curricula.[102]

Proposal 7–4 The Office of the Privacy Commissioner should educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed.

Guidance on particular technologies

Background

7.82 As discussed in Chapter 15, principles-based regulatory schemes require the issuing of guidance that clarifies the rights and obligations contained in the legislation. Chapter 6 examines a number of developing technologies that may require such guidance when used by agencies and organisations to handle personal information.[103] For example, RFID systems, surveillance devices and internet software could allow an agency or organisation to collect personal information about an individual without his or her knowledge or consent. Security issues may arise when information is transmitted by wireless technologies, and large quantities of information are stored electronically. It may also be difficult for an individual to gain meaningful access to personal information that an organisation holds in an encrypted form.

7.83 Agencies and organisations using such technologies to handle an individual's personal information may be required to do certain things to meet the obligations set out in the proposed UPPs. Guidance issued by the OPC—for example, technologically specific guidelines—could specify what is required to fulfil the obligations in the proposed UPPs when personal information is handled by a particular technology.

7.84 In Chapter 44, the ALRC discusses the power of the OPC to prepare guidelines that assist agencies and organisations to avoid acts or practices that may be

---

102 See Proposal 59–4. In Ch 59, the ALRC discusses different attitudes to privacy held by members of different generations.

103 In Ch 64, the ALRC proposes that ACMA, in consultation with the OPC, Australian Communications Alliance and the Telecommunications Industry Ombudsman should develop and publish guidelines that address issues raised by new telecommunications technologies such as location-based data, VoIP and electronic number mapping: Proposal 64–3.

interferences with, or affect adversely, the privacy of individuals. The OPC has used this power to issue guidelines that deal with the data-matching activities of agencies.[104] While guidelines such as these are not binding, they indicate the OPC's understanding of the requirements set out in the UPPs. Guidelines, therefore, can provide greater detail than high level principles, help to modify behaviour and be highly persuasive in the complaint-handling process. The OPC may also take into account compliance with guidelines when conducting an audit.[105]

7.85 The OPC's function to research and monitor technology could provide the OPC with the expertise to develop, in consultation with relevant stakeholders, guidance for personal information handled using particular technologies. In formulating such guidance, the OPC could examine similar guidelines published in other jurisdictions. For example, in June 2006, the Information and Privacy Commissioner Ontario issued *Privacy Guidelines for RFID Systems*. These guidelines are not mandatory, but encourage agencies and organisations to comply with certain limits on collection, use and disclosure of information collected by RFID tags embedded in retail items.[106] In the United States, guidelines issued in April 2007 by NIST outline several steps that could be taken to protect the security of information handled by RFID systems.[107]

7.86 In IP 31, the ALRC asked whether the privacy principles should be amended to deal with the impact of developing technology on privacy.[108] The next section discusses a number of requirements that, in the view of the ALRC, should not be set out in the proposed UPPs, but which could form the subject of technologically specific guidance.

Setting out requirements in the proposed UPPs

Collection

7.87 The proposed 'Collection' principle requires an agency or organisation to collect information only by fair means, and not in an unreasonably intrusive way.[109] Guidance issued by the OPC could explain the meaning of the terms 'fair means' and 'unreasonably intrusive' in relation to certain technologies. This may be required where technologies allow the collection of information without the knowledge of an individual.

7.88 For example, an 'unreasonably intrusive' collection of information by RFID systems might involve collection of information from a RFID tag combined with a

---

104 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998).

105 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5.

106 Information and Privacy Commissioner of Ontario, *Privacy Guidelines for RFID Information Systems* (2006).

107 United States Department of Commerce—National Institute of Standards and Technology, *Guidelines for Securing Radio Frequency Identification (RFID) Systems: Recommendations of the National Institute of Standards and Technology*, Special Publication 800–98 (2007).

108 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.125]–[11.140].

109 See the proposed 'Collection' principle set out at the beginning of this Discussion Paper.

location detection sensor embedded in an item of clothing sold by a retailer. In addition, collection of information by keystroke software installed on internet café computers may not fall within the definition of 'fair means'.

Specific notification

7.89 The ALRC received limited support for requiring agencies and organisations that use certain technologies to collect personal information to comply with additional notice requirements. In the ALRC's view, including such requirements in the proposed 'Specific Notification' principle is not consistent with the high level, technologically neutral approach proposed in this Discussion Paper. [110]

7.90 This could, however, form the subject of technologically specific guidance on the Specific Notification principle. For example, organisations using RFID technology could be required to inform individuals how to remove or deactivate an RFID tag embedded in a product. In addition, agencies and organisations using biometric systems could be required to inform individuals of the error rates of the systems, and the steps that can be taken by an individual wishing to challenge the system's results.[111] Further, guidance could encourage agencies or organisations to inform individuals of the format in which personal information may be disclosed, for example, whether it will be disclosed in an electronic format.

Data security

7.91 The proposed 'Data Security' principle requires agencies and organisations to take reasonable steps to protect personal information from loss, misuse and unauthorised access, modification or disclosure.[112] In relation to the IPPs and the NPPs that deal with data security, the OPC has indicated that what are reasonable steps will depend on: the sensitivity of the personal information held; the circumstances in which the personal information is held; the risks of unauthorised access to the personal information; the consequences to the individual of unauthorised access; and the costs of security systems.[113]

7.92 In Chapter 25, the ALRC proposes that the OPC provide guidance about the meaning of the term 'reasonable steps' in the 'Data Security' principle. This guidance should refer to technological developments in this area and, in particular, relevant encryption standards.[114] In addition, the ALRC proposes that the OPC provide guidance about what is required of an agency or organisation to destroy or render non-

---

110 See Proposal 7–1 and 15–1.

111 See Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), 11.

112 See the proposed 'Data Security' principle set out at the beginning of this Discussion Paper.

113 *Privacy Act 1988* (Cth) s 14, IPP 4; sch 3, NPP 4.1; Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001), 1.

114 Proposal 25–3.

identifiable personal information, particularly when that information is held or stored in an electronic form.[115]

Access and correction

7.93 The proposed 'Access and Correction' principle provides individuals with a general right to access personal information about them that is held by organisations.[116] In IP 31, the ALRC noted that some personal information may be stored in a way that makes it difficult to analyse or comprehend.[117] The European Parliament *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) requires personal information to be communicated to an individual in an 'intelligible form'.[118] This could mean, for example, that a machine capable of reading biometric information, or an expert with the ability to interpret the results of a machine's analysis of biometric information, should be made available to an individual seeking to exercise his or her right of access to this type of personal information.[119]

7.94 The OPC submitted that individuals should have a right to access information in an intelligible form where this is practicable:

> it may be the case that the only information held by the organisation is a biometric template of the individual which exists as a set of numbers and cannot be converted into an image or more meaningful product.

7.95 Further, the OPC submitted that:

> Where it is impracticable for the information to be presented in an intelligible form, an individual should have access to information explaining for instance that the organisation holds a template of one of his or her biometrics and what that template refers to (for example, the face or left index finger).[120]

ALRC's view

7.96 It is implicit in the proposed 'Access and Correction' principle that, where an individual requests access to personal information about him or her that is held by an organisation, the organisation should provide access to the information in an intelligible form where this is practicable. Moreover, the ALRC notes that it is best practice for organisations to hold some information only in encrypted form. For example, the sensitive nature of biometric information—and the difficulty of replacing such information if it is compromised—means that an organisation should destroy the raw data, such as digital photographs, that are obtained when an individual enrols in a

---

115 Proposal 25–6.

116 See the proposed 'Access and Correction' principle. Ch 12 discusses the access and correction requirements for information about an individual that is held by agencies.

117 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [11.132].

118 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12(a).

119 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [82].

120 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

biometric system.[121] Drafting the proposed 'Access and Correction' principle in line with the OPC's submission, therefore, would be undesirable as well as unnecessary. Requiring organisations to provide an individual with information held about them in an intelligible form may encourage organisations to hold certain information, which for security reasons should be encrypted permanently, in an unencrypted form or a form that is able to be decrypted.

7.97 On balance, therefore, the ALRC's view is that the 'Access and Correction' principle should not be drafted to provide individuals with a right to access information in an intelligible form. The OPC should provide guidance about the type of information that an agency or organisation should make available to an individual when information is held in an encrypted form. This could include, for example, information about whether an encrypted biometric template is a facial or fingerprint biometric.

7.98 The ALRC also notes that the proposed 'Access and Correction' principle requires an organisation to take reasonable steps to correct personal information about an individual when that individual establishes that information held by the organisation is not accurate, complete, up-to-date or relevant.[122] For example, if an organisation's biometric system repeatedly fails to identify or authenticate an individual who had provided the organisation with biometric information to enrol in the system, this indicates that the biometric information held by the organisation is not accurate, complete or up-to-date. In this context, it would be 'reasonable' for the organisation to re-enrol that individual in the biometric system.[123]

Automated decision review mechanisms

7.99 In IP 31, the ALRC asked whether an additional privacy principle was required for automated decision-making processes. The ALRC noted that art 15(1) of the EU Directive reflects concern about the increasing automisation of decisions that affect individuals.[124] It states:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[125]

---

121 See, eg, Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Principle 11.

122 See Ch 26.

123 Biometric systems are discussed in detail in Ch 6.

124 L Bygrave, 'Minding the Machine: Art 15 of the EC Data Protection Directive and Automated Profiling' (2000) 7 *Privacy Law & Policy Reporter* 67, 68.

125 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 15(1).

7.100 A person may be subjected to a decision of this kind, however, if the decision is made in certain contractual contexts, or is authorised by a law that also lays down measures to safeguard the data subject's legitimate interests.[126] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under art 29 of the EU Directive, commented that

> where the purpose of the transfer [of personal information] is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[127]

7.101 In the United Kingdom, a data controller, on request in writing by an individual, is required 'to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data'.[128]

7.102 In 2004, the Administrative Review Council (ARC) published a report that contains a number of principles for agencies carrying out automated decision-making processes, and included a principle that provided for the manual review of decisions in certain circumstances.[129] The ARC Report was the basis for a guide published in February 2007 by the Australian Government Information Management Office (AGIMO).[130] This guide provides suggestions on when automated systems may be suitable for administrative decision making, the development and governance of automated systems and the design of such systems.

7.103 Research into computer systems indicates that such systems are not inherently accurate and reliable. Dr Cameron Spenceley notes that the reliability of computer hardware 'is governed not only by the validity and integrity of its design, but also by the lifespan of its physical components'.[131] Further, Spenceley states that the 'proposition that the reliability of computer software generally meets or exceeds some threshold is not demonstrable on an inherent or empirical basis with information and data that are generally available'.[132]

Submissions and consultations

7.104 Two stakeholders addressed whether there should be a privacy principle on automated decision making. The OPC submitted that:

---

126 Ibid, art 15(2).

127 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998, Ch 1.

128 *Data Protection Act 1998* (UK) s 12(1).

129 Administrative Review Council, *Automated Assistance in Administrative Decision Making*, ARC 46 (2004), Principle 22.

130 Australian Government Information Management Office, *Automated Assistance in Administrative Decision-Making Better Practice Guide* (2007).

131 C Spenceley, 'Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation', *Thesis*, University of Sydney, 2003, 121.

132 Ibid 151.

> Currently, individuals are offered some protections through data quality and access and correction principles. However, the Office would support the clarification of the privacy principles to ensure that review mechanisms for automated decisions are a requirement under the Privacy Act.
>
> The Office notes that sometimes review mechanisms will involve the human checking of automated decisions but believes that there may be occasions where a review of a decision will include further automated processes or a combination of human and automated processes. The Office takes the view that, in the interests of technological neutrality, it will [be] important for the Privacy Act both to support fair and reasonable review mechanisms and allow for technological development which enables effective review via automated systems.[133]

7.105 Another submission stated that the ALRC should consider the introduction of a privacy principle that requires human intervention before any adverse action is taken on the sole basis of an automated process.[134]

ALRC's view

7.106 The ALRC supports the practice of human review of decisions that are made by automated means, particularly when an agency or organisation plans to take adverse action against an individual on the basis of such a decision. In supporting this practice, the ALRC notes research that indicates that computer software and hardware may not necessarily produce accurate and reliable results.

7.107 The ALRC has not received sufficient feedback, however, to propose that the UPPs include a prescriptive requirement for agencies and organisations to provide processes for human review of automated decisions. As discussed in Chapter 15, the proposed UPPs generally provide high-level and outcomes-based requirements. The proposed 'Data Quality' and 'Access and Correction' principles in the UPPs provide for outcomes that could be relevant to such a requirement. On balance, therefore, the ALRC has formed the preliminary view that human review of automated decision-making processes should be the subject of guidance issued by the OPC. Such guidance could be based on the material on automated decision-making processes produced by the ARC and AGIMO. In making this proposal, the ALRC notes that ensuring that accurate decisions are made about individuals is in the interests of the agencies and organisations that make such decisions.

Data-matching

7.108 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest'.[135] Privacy

---

133 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

134 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

135 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].

concerns over data-matching include the: revealing of previously unknown information about an individual without the knowledge or consent of that individual; profiling of an individual; difficulty for an individual in accessing information contained in the new data-set without knowledge that such a data-set was compiled; accuracy of the matched data; and the security of large amounts of data collected for the purposes of data-matching or data mining.[136] The impact on privacy of data-matching is discussed further in Chapter 6. Currently, agencies that conduct data-matching activities are subject to some regulation. As discussed in Chapter 27, data-matching activities of organisations may be subject to some of the privacy principles. This section considers whether greater regulation of data-matching activities is required.

Regulation of data-matching

7.109 The Privacy Commissioner has functions relating to data-matching, including undertaking research and monitoring developments in data processing and computer technology (including data-matching and data linkage) to help minimise any adverse effects of such developments on privacy.[137] In addition, the Privacy Commissioner can examine (with or without a request from a Minister) any proposal for data-matching or data linkage that may involve an interference with privacy or that may have any adverse effects on the privacy of individuals.[138] The Privacy Commissioner may report to the Minister (currently the Attorney-General)[139] about the results of any research into developments in data-matching or proposals for data-matching.[140]

7.110 As discussed in Chapter 27, the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *Data-matching Program (Assistance and Tax) Guidelines* (the Guidelines) regulate the use of tax file numbers to match data held by certain agencies, such as the Australian Taxation Office and Centrelink. The Privacy Commissioner monitors compliance with the Act and the Guidelines. The Privacy Commissioner advises agencies about the interpretation of the Act and inspects the way in which they undertake data-matching regulated by the Act.[141] An act or practice that breaches Part 2 of the *Data-matching Program (Assistance and Tax) Act*, or the Guidelines, constitutes an 'interference with privacy'.[142] An individual can complain to the Privacy Commissioner about any such act or practice.[143]

7.111 Agencies may also engage in data-matching activities that do not involve the use of tax file numbers. For example, in early 2004 ASIC began matching data from its public database with data from the Insolvency and Trustee Service Australia's National

---

136 See Ch 7.
137 See *Privacy Act 1988* (Cth) s 27(1)(c).
138 Ibid s 27(1)(k).
139 Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.
140 *Privacy Act 1988* (Cth) ss 27(1)(c), 32(1).
141 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), [3.8].
142 *Privacy Act 1988* (Cth) s 13.
143 Ibid s 36; *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 14.

Personal Insolvency Index.[144] The purpose of this data-matching program is to identify individuals who should be disqualified automatically from managing corporations under the *Corporations Act 2001* (Cth).[145]

7.112 The Privacy Commissioner has issued guidelines for agencies that engage in data-matching practices that are not regulated by the *Data-matching (Assistance and Tax) Act 1990* (Cth) (the voluntary data matching guidelines).[146] The voluntary data matching guidelines aim to ensure that data-matching programs 'are designed and conducted in accordance with sound privacy practices'.[147] Although the guidelines are not legally binding, a number of agencies have agreed to comply with them.[148]

7.113 The voluntary data matching guidelines apply to agencies that match data from two or more databases if at least two of the databases contain information about more than 5,000 individuals.[149] In summary, the guidelines require agencies to: give public notice of any proposed data-matching program; prepare and publish a 'program protocol' outlining the nature and scope of a data-matching program; provide individuals with an opportunity to comment on matched information if the agency proposes to take administrative action on the basis of it; and destroy personal information that does not lead to a match. Further, the voluntary data matching guidelines generally prohibit agencies from creating new, separate databases from information about individuals whose records have been matched.[150]

7.114 In IP 31, the ALRC asked whether data-matching programs that fall outside the *Data-matching Program Assistance and Tax Act* should be regulated more formally.[151]

Submissions and consultations

7.115 A number of stakeholders stated that agencies should be subject to greater regulation when conducting data-matching programs. The OPC submitted that:

> In light of the expanding capacity to conduct widescale data manipulation in timely and cost effective ways, the Office recommends that consideration be given to making the voluntary public sector data matching guidelines mandatory. In making the

144 Australian Securities and Investments Commission, *ITSA Data Matching Protocol* <www.asic.gov.au> at 31 July 2007.
145 Ibid.
146 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997).
147 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 1.
148 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 68–71.
149 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [15].
150 Ibid, [33]–[41], [42]–[47], [63], [69].
151 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(h).

> guidelines enforceable, the Office notes that they may require reviewing to bring them in line with current practices and new technologies.[152]

7.116 The Australian Privacy Foundation also submitted that agencies should be subject to mandatory data-matching rules based on the OPC guidelines, although the Foundation was 'indifferent to whether this is effected through the Data-matching or Privacy legislation'.[153]

7.117 The Office of the Victorian Privacy Commissioner submitted that data-matching should be specifically addressed, 'preferably by separate data-matching provisions'.[154] The Centre for Law and Genetics stated that 'modern technology enables sophisticated data matching and it may be timely for there to be a separate principle on this issue'.[155] Similarly, the Queensland Government submitted that there was a

> need for privacy principles dealing with data-matching, and related processes where data is used by other parties or in ways not anticipated when the information was originally collected … controlling the level of aggregation of specific de-identified data items—for example, using age ranges rather than specific ages or dates of birth—would address this issue to ensure de-identified data items do not allow individuals to be reasonably identified.[156]

7.118 In addition, the Queensland Government submitted that:

> Competing with these privacy interests are the demands of administrative efficiency, including the need to reduce the burden of data collection for respondents and collection agencies, and the need to cater for re-use of administrative data for statistical purposes. Any privacy principle dealing with data-matching ought to be tempered with recognition of the need for statistical and administrative efficiency.[157]

7.119 A number of stakeholders submitted that the privacy principles do not regulate adequately the data-matching activities of organisations. The Office of the Information Commissioner Northern Territory submitted that:

> NPP 2 and IPP 11 regulate the disclosure of information for the purposes of data-matching by an agency or organisation. NPP 7 currently provides a limitation on the facilitation of data-matching by use of an identifier assigned by another. However, other principles regarding collection of personal information do not present significant checks on collection of information for data-matching purposes.[158]

7.120 The Office of the Victorian Privacy Commissioner noted that data-matching 'occurs across federal, state and territory government agencies and across public and private sectors within Australia and overseas'.[159] Similarly, the OPC submitted that:

---

152 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
153 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
154 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
155 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
156 Queensland Government, *Submission PR 242,* 15 March 2007.
157 Ibid.
158 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
159 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

> As the necessary technology becomes widely available, there is likely to be significant potential for increased data matching in the private sector. In the Office's view, private sector data matching activity might be an area best dealt with under a binding code making power for the Privacy Commissioner.[160]

7.121 It was suggested in another submission that:

> The Discussion Paper should give consideration to the inclusion of a definition of 'data matching' and to empowering the Privacy Commissioner to regulate all data matching practices according to a set of statutory principles. Consideration should be given to whether such regulation should also apply to the private sector.[161]

ALRC's view

7.122 It would appear from the information provided to the ALRC in this Inquiry that agencies are complying with the voluntary data-matching guidelines issued by the OPC. The ALRC does not propose, therefore, that these guidelines be made mandatory. The ALRC notes that the OPC has the function to research and monitor technology, including data-matching, and report the result to the Minister.[162] The OPC submitted that the data-matching guidelines should be reviewed if they were made mandatory. In the ALRC's view, the OPC could review the existing guidelines if the OPC deems this to be necessary.

7.123 The ALRC notes, however, that stakeholders indicated that the application of the privacy principles to the data-matching activities of organisations was not clear.[163] Further, there is currently no OPC guidance that applies to organisations engaged in data-matching. The ALRC's view is that the OPC should issue guidance that applies to data-matching by organisations. This guidance could be in the form of guidelines that are based on the existing data-matching guidelines that apply to agencies.

7.124 In addition, in Chapter 44 the ALRC proposes that the OPC should be empowered to request the development of a privacy code, and to develop and impose a privacy code that applies to designated agencies and organisations.[164] The ALRC's view is that this mechanism could be used to regulate more prescriptively the data-matching activities of agencies and organisations if the OPC deems this to be necessary.

---

160 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
161 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
162 *Privacy Act 1988* (Cth) s 27(1)(c).
163 See also the discussion of data-matching in relation to the proposed 'Identifiers' principle in Ch 27.
164 Proposal 44–10.

Proposal 7–5 The Office of the Privacy Commissioner should provide guidance in relation to technologies that impact on privacy (including, for example, guidance for use of RFID or data collecting software such as 'cookies'). Where appropriate, this guidance should incorporate relevant local and international standards. The guidance should address:

(a) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';

(b) when the use of a certain technology will require, under the proposed 'Specific Notification' principle, agencies and organisations to notify individuals at or before the time of collection of personal information;

(c) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometrics systems);

(d) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information held in an intelligible form (for example, what biometric information is held about an individual when the information is held as an algorithm); and

(e) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

Proposal 7–6 The Office of the Privacy Commissioner should provide guidance to organisations on the privacy implications of data-matching.

Co-regulation

7.125 The *Privacy Act* currently provides, through the OPC's power to approve privacy codes, a form of co-regulation for agencies and organisations that develop and deploy particular technologies.[165] In effect, privacy codes replace the privacy principles. Once a privacy code has been developed by an industry and approved by the OPC, the requirements set out in the code are binding on organisations that have agreed to be bound. Further discussion of the operation of the current code-making power and the co-regulatory nature of privacy codes is contained in Chapter 44.

7.126 In Chapter 44, the ALRC proposes that the OPC be empowered to request the development of a privacy code; and develop and impose a privacy code that applies to

165 *Privacy Act 1988* (Cth) pt IIIAA.

designated agencies and organisations.[166] This section provides an overview of two codes that could inform the OPC's exercise of these proposed powers.

Internet Industry Association Draft Code

7.127 The Internet Industry Association (IIA) has expressed the view that government regulation of privacy on the internet is problematic because the process of making new laws is too slow to deal adequately with developments in technology.[167] Accordingly, it believes that co-regulation between government and businesses in relation to privacy issues is 'a flexible way of maintaining relevant and enforceable best practice standards within a rapidly changing communications environment'.[168]

7.128 In 2003, the IIA lodged a draft privacy code with the OPC for approval under s 18BB of the *Privacy Act*.[169] If approved, the code will apply to members of the IIA who: (i) agree to be bound by it; and (ii) provide services on or through the internet from a location within Australia; are engaged in an internet related business; or are directly or indirectly commercially interested in the internet.[170]

7.129 The code aims to close a number of gaps in the existing privacy regime. It may apply to small business operators who are currently exempt from the operation of the *Privacy Act*.[171] It may also apply when personal information is included in an employee record or is collected for inclusion in a generally available publication.[172] The code, however, would not apply to individuals dealing with personal information in their personal capacity.[173]

Biometrics Institute Code

7.130 On 27 July 2006, the Privacy Commissioner announced the approval of the *Biometrics Institute Privacy Code*.[174] The preamble to the Code notes that 'Biometrics Institute members understand that only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance'.[175] The Code binds Biometrics Institute members who sign the Biometrics Institute Privacy

166 Proposal 44–10.
167 Internet Industry Association, *What is Co-regulation?* (1998) <www.iia.net.au> at 31 July 2007.
168 Ibid.
169 Privacy codes are discussed further in Ch 6.
170 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001).
171 See, however, the ALRC's proposal that the *Privacy Act* should be amended to remove the small business exemption: Proposal 35–1.
172 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001).
173 Ibid.
174 K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).
175 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Preamble, [2].

Code Agreement to Comply.[176] To date, four organisations have agreed to be bound by the Code.[177]

7.131 The Code aims to: (i) facilitate the protection of personal information provided by, or held in relation to, biometric systems; (ii) facilitate the process of identity authentication in a manner consistent with the *Privacy Act* and the NPPs; and (iii) promote biometrics as PETs.[178] It includes information privacy standards that are at least equivalent to the NPPs.[179] In addition, it requires organisations that have agreed to be bound by the Code to observe higher levels of privacy protection than those in the NPPs in certain circumstances. For example, the Code applies to acts and practices relating to employee records that are exempt from the operation of the *Privacy Act* if a biometric is included as part of the employee record, or has a function related to the collection and storage of, access to, or transmission of an employee record.[180]

7.132 The Code also contains three new information privacy principles. Principle 11 (Protection) sets out the steps that Code subscribers must take to protect biometric information, including ensuring that biometric information is de-identified where practicable, only stored in encrypted form and is not held in a way that makes it easy to match to other personal information. Principle 12 (Control) requires enrolment in biometric systems to be voluntary, and prevents organisations from using biometric information for some secondary purposes without 'free and informed consent'. Principle 13 (Accountability) requires individuals to be informed of the purposes for which a biometric system is being deployed. It also requires biometric systems to be audited and Code subscribers to adopt a holistic approach to privacy policy and procedures. Finally, it mandates the use of privacy impact assessments as part of the planning and management process for biometrics implementation.

Other regulatory mechanisms

7.133 The ALRC is interested in hearing whether the mechanisms proposed in this chapter provide an adequate and effective framework for addressing the impact of developing technology on privacy. In particular, the ALRC is interested in hearing about any effective regulatory mechanisms that have not been considered in this chapter.

176 Ibid, [C.1], [C.2].
177 Biometrics Institute, *Biometrics Institute Privacy Code—Public Register* (2006) <www.biometricsinstitute.org> at 3 August 2007.
178 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [B.1].
179 K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).
180 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [D.5].

8. Individuals, the Internet and Generally Available Publications

Contents

Introduction 375
Individuals acting in a personal capacity 376
Submissions and consultations 376
Take down notices for online content 378
Other options for reform 380
ALRC's view 381
Generally available publications 383
Application of the *Privacy Act* 384
Public registers 385
Court records 386
Submissions and consultations 387
Options for reform 389
ALRC's view 390

Introduction

8.1 The *Privacy Act 1988* (Cth) does not regulate the handling of personal information by individuals for the purposes of, or in connection with, their personal, family or household affairs.[1] This means that an individual acting in a personal capacity—for example, an individual who posts personal information about others on a personal 'blog'—is not regulated by the *Privacy Act.* In addition, the privacy principles apply to personal information that is *collected* by an agency or organisation for inclusion in a record or a generally available publication but not to personal information that is *held* in a generally available publication—only to personal information held in a 'record'. Publications that are generally available, including publicly accessible websites, are not 'records' for the purposes of the *Privacy Act.*[2]

8.2 The application of the *Privacy Act* is also limited by a number of provisions that excuse an agency or organisation from complying with specific privacy principles in certain circumstances.[3] For example, some small business operators that are not bound by the *Privacy Act*, such as some internet service providers (ISPs) handle large

1 *Privacy Act 1988* (Cth) ss 7B(1), 16E.
2 Ibid s 6(1).
3 All private and public sector exemptions are examined in detail in Part E.

amounts of personal information. It has been estimated that approximately 25% of ISPs in Australia fall within the small business exemption in the *Privacy Act*.[4] In Chapter 35, the ALRC proposes that the *Privacy Act* be amended to remove this exemption.[5]

8.3 This chapter discusses concerns about two other limitations of the *Privacy Act* given developments in technology and, in particular, the internet. The chapter first discusses whether the *Privacy Act* should regulate individuals who publish information in the online environment. The chapter then discusses whether the *Privacy Act* needs to be amended to address issues about generally available publications in electronic form.

Individuals acting in a personal capacity

8.4 A major concern about individuals handling personal information relates to the content of information published on the internet. For example, individuals can monitor the online activities of others through the use of spyware.[6] One submission to the Inquiry noted that emails sent to multiple people may disclose to each other the email addresses of all of the recipients.[7] In addition, individuals regularly use social networking and user-generated sites such as Facebook and YouTube to post photographs, videos and commentary that may interfere with the privacy of other individuals.[8] Further, it has been estimated that there are at least 100 websites that contain images of people caught showering or undressing.[9]

8.5 Currently, a procedure exists for removing offensive or illegal content that is accessible via the internet.[10] There is no similar procedure, however, for removing other privacy-invasive information published on the Web by an individual acting in his or her non-business capacity.

Submissions and consultations

8.6 The Australian Communications and Media Authority (ACMA) submitted that 'the suppliers of content on the web are increasingly individuals who are not, in the

---

4 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 56.

5 See Proposal 35–1 and accompanying text. Other exemptions are discussed in Part E.

6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 244.

7 J Partridge, *Submission PR 26,* 4 June 2006.

8 See, eg, P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>. Also see discussion in Ch 59.

9 C Calvert, *Voyeur Nation: Media, Privacy, and Peering in Modern Culture* (2000), cited in D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 100.

10 The Australian Communications and Media Authority (ACMA) can investigate complaints about content available via the internet. If satisfied that content is hosted in Australia and is 'prohibited content'—namely, content that has been given a certain classification by the Classification Board—or potentially prohibited content, ACMA must direct the relevant internet content host to remove the content: see *Broadcasting Services Act 1992* (Cth) sch 5.

main, regulated in any way by current privacy provisions'.[11] Similarly, the Legal Aid Commission of NSW submitted that:

> the Internet creates an environment where responsibility for protection of personal information should be spread as widely as possible, and not limited to commercial and administrative users.[12]

8.7 One individual advised the Inquiry that extensive personal information about herself and several family members has been published on an amateur genealogy website since late 2006. The information was posted without the knowledge or consent of the relevant individuals. She noted that she had unsuccessfully requested both the individual that owned the website and the relevant ISP to remove the information but 'there is no one with the authority … to discover the source of this information or to have the information removed from the website'.[13]

8.8 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* should be amended to cover any acts or practices of individuals relating to their personal, family or household affairs.[14] The majority of submissions did not support an expansion of the scope of the *Privacy Act* to regulate individuals acting in a non-commercial capacity. For example, Electronic Frontiers Australia submitted that the *Privacy Act* is not 'an appropriate vehicle for application to the acts or practices of individuals relating to their personal, family or household affairs'. This was because it would be 'impractical and undesirable' to require individuals acting in a private capacity to comply with the requirements in the privacy principles.[15] Electronic Frontiers Australia submitted further that:

> the primary issues of concern are publication and/or public distribution and that collection and private use of information is generally of significantly less concern except under some particular circumstances.[16]

8.9 Similarly, the Office of the Privacy Commissioner (OPC) submitted that:

> the Privacy Act has been specifically tailored to regulate agencies and organisations and as such is ill-suited to the regulation of individuals in their personal capacity. For instance, it would be difficult and undesirable to require individuals to give notice or seek consent for collection of personal information. Also, applying data quality and data security principles to an individual's address book could be inappropriate.[17]

---

11 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.
12 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
13 J Watts, *Submission PR 302,* 10 July 2007.
14 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 11–2(a).
15 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
16 Ibid.
17 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

Take down notices for online content

8.10 One method to deal with the issues associated with the user-generated nature of Web 2.0[18] is to broaden the scope of the existing 'take down' notice scheme that deals with internet content.[19] ACMA administers the co-regulatory scheme, which relies on the classification decisions of the Classification Board to determine what is prohibited content.[20] While it is not an offence to host prohibited content, if ACMA acts on a complaint and issues a take down notice to an internet content host, the prohibited content must be removed as soon as practicable or, at the latest, by 6pm the next business day. Potential prohibited content can be the subject of an interim take down notice while waiting for the outcome of classification. This is important as, in practice, internet content is not classified until ACMA, acting on a complaint, refers the material to the Classification Board to be classified in the same way as a film or computer game.

8.11 The RC (refused classification) classification covers content that describes or depicts in a way that is likely to cause offence to a reasonable adult a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not).[21] When undertaking classification, the Classification Board can take into account the context in which an image appears. For example, the Classification Board has previously classified as RC (and therefore prohibited content) an inoffensive image of a five year old child fully clothed on a web page with an offensive URL.[22]

8.12 As with any scheme regulating online content, the online content classification scheme has jurisdictional limitations. If the internet content is hosted outside Australia, ACMA is unable to issue a take down notice. If sufficiently serious, however, ACMA can refer a matter to law enforcement authorities. ACMA can also refer the matter to ISPs to take appropriate technical steps to minimise access to the material by end-users in Australia.[23]

---

18 The term 'Web 2.0' can be used in various contexts. In this Discussion Paper, it is used to refer to the social phenomenon where internet users—often individuals acting in a personal capacity—upload and distribute content such as text, photographs and videos.

19 The online regulation scheme is set out in *Broadcasting Services Act 1992* (Cth) sch 5. The current scheme focuses on stored content made available over the internet. The *Communications Legislation Amendment (Content Services) Act 2007* (Cth), due to commence operation in January 2008, will expand the scheme to cover live streamed content services, mobile phone-based services and services that provide links to content, and move the entire online content scheme to a new schedule 7 of the *Broadcasting Services Act 1992* (Cth).

20 Content that is, or would be, classified as RC or X18+, or is classified R18+ and not subject to an appropriate age-restricted access system that complies with the criteria determined by ACMA, is considered to be prohibited internet content: *Broadcasting Services Act 1992* (Cth) sch 5, cl 10.

21 *National Classification Code* (2005). There are other aspects of the RC classification focused on matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena.

22 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), 21–22. The SCAG paper identified a small gap in existing classification laws in relation to considering both the image and the text of website links. This issue will not be addressed by the ALRC.

23 *Broadcasting Services Act 1992* (Cth) sch 5, cl 40.

8.13 In its current format, the take down notice scheme cannot be used for making general complaints regarding internet content and concerns about invasion of privacy. The existing scheme's dependence on the *National Classification Code* and decisions of the Classification Board limits the extent to which the take-down notice procedure can be used. It is essentially an extension of the censorship scheme into the online environment and balances a number of competing interests.

> In relation to freedom of expression, Schedule 5 is premised on the principle that what is illegal offline should also be illegal online. It does not provide for more onerous restrictions than those that apply to conventional media regulated under the Act. Definitions of prohibited material are based on specific and detailed criteria of the widely accepted national classification scheme administered by the Office of Film and Literature Classification. This scheme is designed to balance the public interest in allowing adults to read, hear and see material of their own choosing, with the public interest in protecting minors from material likely to harm or disturb them, and in protecting the community generally from offensive material.[24]

8.14 A 2004 review of the operation of the scheme found that it had clear community support, in particular for the existing complaints mechanism, the co-regulatory framework including the industry codes of practice, and the community education element of the scheme.[25] While some suggestions for change were made, the basic framework of the scheme was left intact, including the dependence on the existing national classification system. One issue raised by the Human Rights and Equal Opportunity Commission was the potential for cyber-racism and the current absence from the classification standards of racially offensive material. The review stressed the underlying policy of the scheme to align internet content regulation with content regulation of offline services, and firmly avoided any move away from the *National Classification Code* as the basis of online content regulation.[26]

8.15 If the take down notice scheme were more closely tied to complaints about invasion of privacy, it could provide an effective remedy not otherwise available for those with concerns about the unauthorised online publication of their personal information, including images. It would be necessary, if the take down notice scheme were extended, to link the complaint about the content with some test that the content be considered to cause substantial offence to a reasonable person—such as the ALRC is considering as one element of a statutory cause of action for invasion of privacy.[27] It is likely, however, that any expansion of the scheme to cover a wider range of content would be opposed by some, particularly on the ground that it undesirably restricts freedom of expression.

---

24 Australian Government Department of Communications Information Technology and the Arts, *Review of the Operation of Schedule 5 to the Broadcasting Services Act 1992: Report* (2004), 14.

25 Ibid, 13. There were, however, a number of submissions opposed to the continuation of the scheme on the grounds of limits to freedom of expression and information technology employment, and the costs of maintaining the scheme: 13–14.

26 Ibid, 37–38.

27 See, Proposal 5–2.

8.16 It should also be noted that, at present, a finding of a criminal offence against a person for publication of offensive material does not necessarily result in the ability to remove the material from the internet via a take down notice. The content must be the subject of an appropriate classification and be considered prohibited content. There are instances where the image itself may be innocuous, and although the taking and use of the image may have been considered a criminal offence, unless the image appears on a website in a context that falls within the guidelines of the *National Classification Code*, the image is unable forcibly to be removed. It seems appropriate that any image, which was taken or published in a manner later found to be the subject of criminal conduct, should be able to be destroyed and, if published, removed from publication, including online publication. The Standing Committee of Attorneys-General (SCAG) is currently considering gaps in the criminal law for the unauthorised taking of photographs and, through this process, could give this issue further consideration.[28]

Other options for reform

Civil litigation

8.17 Another way to address the issues arising from individuals acting in their non-commercial capacity—in particular, when individuals add content to websites—is to introduce into the *Privacy Act* a statutory cause of action. The OPC submitted that this 'may go some way to providing individuals with an avenue for redress in the event that their privacy was interfered with by an individual acting in a personal capacity'.[29]

8.18 Electronic Frontiers Australia supported the introduction of a cause of action for invasion of privacy as one alternative to expanding the scope of the *Privacy Act* to regulate individuals acting in a non-commercial capacity.[30] On the other hand, the Legal Aid Commission of NSW submitted that:

> Unfortunately litigation only further publicises the privacy breach. If the function of privacy legislation is to provide practical and privacy sensitive remedies in response to the invasive impact of new technologies, then there is no overwhelming reason to limit its scope to commercial and administrative activities. However, different compliance standards and different kinds of remedial action may be necessary if the Act was extended to cover the way individuals use personal information.

8.19 Electronic Frontiers Australia also suggested the introduction of legislation that grants 'individuals rights to control use of their image'.[31] The Arts Law Centre of Australia noted the interests of 'privacy versus freedom of expression' but submitted that:

> there should also be a consideration of how any further restrictions on creating art, photographs or films in public further privatises public space, and limits the capacity of artists to make art in a public context. This genre of art is important as it reflects, records and explores public places and spaces and those people who inhabit them.

---

28 The SCAG deliberations are discussed later in this chapter and in Ch 59.
29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
30 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
31 Ibid. Property-based schemes are discussed in Ch 7.

Criminal legislation

8.20 In certain situations, legislation that prohibits certain acts and practices of individuals may be an alternative to commencing a potentially expensive and privacy invasive civil action. For example, in August 2005, SCAG released a discussion paper on the unauthorised publication of photographs on the internet.[32] It noted that the small size of cameras and the advent of mobile telephone cameras made it easier to take photographs of others without their knowledge or consent.[33] It also noted that the unauthorised publication of photographs on the internet highlighted a tension between privacy and freedom of expression.[34] Several options for reform were suggested, including criminalising the unauthorised publication of photographs of children on the internet.[35]

8.21 Electronic Frontiers Australia submitted that another way to deal with the impact on privacy of some new and emerging technologies could be to make individuals subject to legislation that prohibits 'specified types of conduct in particular circumstances'.[36] Similarly, the Australian Privacy Foundation submitted that:

> objectionable practices by individuals such as voyeuristic photography, internet publication of unwelcome information about another individual etc are best dealt with by other civil law measures, including a tort of privacy, and criminal laws where appropriate …[37]

8.22 On the other hand, the Australian Press Council submitted that the proposals made in SCAG's discussion paper

> might result in repressive restrictions on taking photos in public places. The ability of photojournalists to record the culture and history of Australia is under threat from such proposals.[38]

ALRC's view

8.23 The ALRC agrees that it is not practical or desirable to expand the scope of the *Privacy Act* to regulate individuals acting in a non-commercial capacity. In reaching this view, the ALRC notes that much of the concern about individuals acting in a non-commercial capacity relates to information posted by individuals on websites. Once an individual posts information on a website, however, the information becomes a

---

32 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005).
33 Ibid, [26].
34 Ibid, [21].
35 Ibid, [6.1.1]–[6.2.2]. Options for reform of unauthorised publication of photographs are discussed further in Ch 59.
36 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
37 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
38 Australian Press Council, *Submission PR 48,* 8 August 2006.

'generally available publication' and is subject to limited protection by the *Privacy Act*.[39]

8.24 The ALRC's view is that there are other methods that could more appropriately deal with situations where an individual acting in a personal capacity interferes with another individual's privacy. In Chapter 5, the ALRC proposes that the *Privacy Act* be amended to include a statutory cause of action.[40] The proposed statutory cause of action may be used against an individual acting in a non-commercial capacity—such as an internet blogger who does not fall within the definition of a 'media organisation'—as well as against an agency or organisation.

8.25 In addition, the ALRC is interested in receiving further input on whether the take down notice scheme should be expanded beyond the existing definitions of prohibited content, and possibly allow for an additional circumstance where the content may constitute an invasion of an individual's privacy. Such a scheme would be useful where an individual refuses to remove from his or her website personal information about another person—for example, an amateur genealogist who has posted personal information on his 'family tree' website. Further, a take down notice scheme could provide a timely remedy and an option for individuals who do not have the means to commence a court action.

8.26 The ALRC notes, however, that even the implementation of the statutory cause of action for invasion of privacy and the take down notice scheme, will not address entirely the inherent difficulties in regulating the use and disclosure of personal information published on the internet. For example, while the *Privacy Act* has extraterritorial application, individuals, agencies and organisations that post information online may be based in other jurisdictions, which may present, in practice, enforcement difficulties.[41] In addition, information posted online can be copied onto an infinite number of other websites within minutes. It may be very time consuming and costly—if not impossible—to remove altogether privacy invasive information from the internet.[42]

8.27 It is necessary to educate individuals, therefore, about the impact on their privacy and that of others that may result from posting online personal information. While online education programs should not be directed only towards children and young people, the ALRC notes the importance of early education on the impact of the internet on privacy. In Chapter 59, the ALRC proposes that, to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curricula.[43]

---

39 The regulation of generally available publications is discussed in the next section of this chapter.

40 Proposal 5–1.

41 *Privacy Act 1988* (Cth) s 5B.

42 A Brown, 'They Know All About You', *Guardian Unlimited Technology* (online), 28 August 2006, <technology.guardian.co.uk>.

43 Proposal 59–4.

Question 8–1 Should the online content regulation scheme set out in the *Broadcasting Services Act 1992* (Cth), and in particular the ability to issue take down notices, be expanded beyond the *National Classification Code* and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take down notice should be issued? What is the appropriate body to deal with a complaint and issue the take down notice?

Generally available publications

8.29 Personal information about a substantial number of people is available from public sources such as electoral rolls, court records, state registers of births, deaths and marriages, annual reports and newspapers. This information may be of interest to people for a multitude of reasons. For example, it may be of interest to: people engaged in direct marketing or fundraising; employers wishing to investigate potential employees; politicians wishing to know more about their constituents or vice versa; people wishing to use false identities to engage in illegal activities; or law enforcement officers investigating criminal offences.

8.30 In the past, individuals seeking to access generally available publications were usually required to attend the location where the information was stored, such as a court house, and to expend a considerable amount of time manually searching or copying records.[44] This meant that generally available publications were afforded a degree of de facto privacy protection. Developments in information and communications technologies, such as the creation of powerful computer databases and the internet, have greatly altered the way in which information is stored, accessed, combined, transferred and searched.[45] In particular, information can now be published in electronic form. While it is arguable that information in the public domain should be available in all formats, it can also be argued that privacy 'can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible'.[46]

8.31 The publication of publicly available information in electronic form increases the ability of third parties to combine disparate pieces of personal information about others.[47] Disparate pieces of information about a person may reveal little when viewed separately, but the aggregation of these pieces of information—for example, in the search results provided by an internet search engine in response to a search query about

---

44 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, 1152.

45 Ibid, 1152–1153.

46 Ibid, 1178.

47 M Neave, 'International Regulation of the Publication of Publicly Accessible Personal Information' (2003) 10 *Privacy Law & Policy Reporter* 120, 122.

a person's name—can provide a detailed profile of a person. Internet search engines and social networking sites may be used by third parties to obtain information about individuals for a number of purposes. For example, a recent United Kingdom study noted that one in five employers searched the internet to find information about job applicants.[48] In addition, personal information about an individual, which is obtained by another person conducting an internet search on that individual, can be used to conduct identity theft.[49] Another issue is that information aggregated from a variety of different publicly available sources may present an inaccurate portrait of an individual if, for example, inaccurate information was collected or errors occurred during the aggregation process.

Application of the *Privacy Act*

8.32 The privacy principles apply to personal information that an agency or organisation collects for the purpose of inclusion in a 'record' and a 'generally available publication'.[50] On the other hand, the privacy principles that deal with the handling of personal information subsequent to collection only apply to personal information that is held in a record.[51] A record is defined as a document, a database, or a photograph or other pictorial representation.[52] A book, magazine or other publication that is generally available to the public is not a record for the purposes of the *Privacy Act*.[53] In the internet context, guidance issued by the OPC indicates that websites that are not encrypted or not password protected are considered 'generally available'.[54]

8.33 There are other restrictions on the handling of personal information contained in a generally available publication. An agency or organisation that continues to hold personal information that has been made generally available in a record—for example, a master copy—will need to comply with the requirements in the privacy principles for the personal information that is held in a record.[55] Moreover, an agency or organisation that collects personal information *from* a generally available publication for inclusion

48 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007).

49 Identity theft is discussed in Ch 9.

50 *Privacy Act 1988* (Cth) s 14, IPPs 1–3 and s 16B(1).

51 Ibid s 14, IPPs 4–11 and s 16B(2). In the credit reporting context, only some categories of publicly available information are permitted to be included in credit information files: *Privacy Act 1988* (Cth) s 18E(1). In Ch 52, the ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information: Proposal 52–6.

52 *Privacy Act 1988* (Cth) s 6(1). In Ch 3, the ALRC proposes that the definition of 'record' should be amended to include (a) a document and (b) information stored in electronic or other forms: Proposal 3–6.

53 Ibid s 6(1). In Ch 3, the ALRC proposes that the definition of a generally available publication should be amended to clarify that a publication is generally available whether or not a fee is charged for access to the publication: Proposal 3–9.

54 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003); Office of the Federal Privacy Commissioner, *Guidelines for Federal and ACT Government Websites* (2003) <www.privacy.gov.au/internet/web/> at 23 July 2007.

55 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003), 3.

in a record or another generally available publication will need to comply with the requirements in the relevant privacy principles.[56]

8.34 This section provides an overview of two sources of publicly available information—public registers and court records.

Public registers

8.35 In the late 19th century, governments began systematically to compile and retain records of their citizens. Today, records are kept 'for almost every occasion an individual comes into contact with the state bureaucracy'.[57] Legislation may require these records to be used to create public registers. For example, the *Commonwealth Electoral Act 1918* (Cth) requires the Australian Electoral Commission to construct and maintain a roll of people eligible to vote at federal, and, by agreement, most state and local government elections. Electoral rolls are available for public inspection without fee at offices of the Australian Electoral Commission.[58]

8.36 Public registers often promote important public interests. For example, a publicly available electoral roll facilitates the conduct of free and fair elections by 'enabling participants to verify the openness and accountability of the electoral process and object to the enrolment of any elector'.[59] There is, however, a tension between the public interests served by a public register of information and privacy of individuals included on the register. This is exacerbated when it is compulsory to provide the information that is included in the register.[60]

8.37 It has been argued that failure to protect adequately the privacy of personal information contained in public registers can have serious consequences. For example,

---

56 See the proposed 'Collection', 'Specific Notification' and 'Data Quality' principles, which are set out at the beginning of this Discussion Paper. In relation to the proposed 'Collection' principle, note in particular the requirements relating to: the collection of personal information about an individual only from that individual if it is reasonable and practicable to do so; and the additional requirements related to the collection of sensitive information. In relation to the proposed 'Specific Notification' principle, note in particular the requirement for an agency or organisation that collects personal information about an individual other than from the individual concerned to take reasonable steps to ensure that the individual has been made aware of the requirements in the proposed 'Specific Notification' principle. This requirement applies in circumstances where a reasonable person would expect to be notified.

57 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, 1143.

58 *Commonwealth Electoral Act 1918* (Cth) s 90A.

59 Australian Electoral Commission, *How to View the Commonwealth Electoral Roll* <www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/How_to_view_electoral_roll.htm> at 31 July 2007.

60 For example, it is compulsory for individuals who are entitled to have their names included on an electoral roll to enrol within 21 days of becoming so entitled: *Commonwealth Electoral Act 1918* (Cth) s 101.

individuals may choose to withdraw from public life in order to protect their privacy.[61] Concern has been expressed that the widespread dissemination of electors' personal information 'has the potential to discourage some electors from enrolling and exercising their democratic rights and duties'.[62] Research conducted for the OPC indicates that only 19% of survey participants believed that businesses should be allowed to use the electoral roll for marketing purposes.[63]

8.38 Legislation establishing a public register can also limit the use and disclosure of information acquired from the register. For example, s 177 of the *Corporations Act 2001* (Cth) prohibits any person from using information collected from a shareholder register to contact a shareholder.[64] Legislation may limit the use and disclosure of information acquired from a register that is published in electronic form. For example, the *Commonwealth Electoral Act 1918* (Cth) prohibits a person from using for commercial purposes electoral roll information provided by the Australian Electoral Commission (AEC) in tape or disk format.[65] In addition, a person cannot disclose electoral roll information provided by the AEC in tape or disk format unless the disclosure is in connection with an election or referendum or monitoring the accuracy of information contained in a roll or other prescribed purpose.[66]

Court records

8.39 The principle of open justice is an essential feature of the common law judicial tradition. It requires the administration of justice to be conducted in open court. The principle of open justice 'is an important safeguard against judicial bias, unfairness and incompetence, ensuring that judges are accountable in the performance of their duties'.[67] In 2006, the New Zealand Law Commission confirmed that the principle of open justice generally requires open access to court records.[68]

8.40 Court records often contain a vast amount of personal information about a number of people, including the parties, family members of the parties, and witnesses. For example, records of bankruptcy cases may include details of the financial circumstances of bankruptees; records of cases in which compensation is sought may include detailed information regarding the health of the plaintiff; records of family court proceedings may contain detailed information about family relationships; and records of criminal cases may include information about an offender's previous criminal history, social security status or mental health.

---

61 See B Givens, *Public Records on the Internet: The Privacy Dilemma* (2002) Privacy Rights Clearinghouse <www.privacyrights.org/ar/onlinepubrecs.htm> at 31 July 2007.

62 Australian Electoral Commission, *Submission to the Joint Standing Committee on Electoral Matters Inquiry into the 2001 Federal Election*, 1 July 2002, Appendix D, 8.

63 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), [6.4].

64 Ch 13 discusses collection of personal information that is required or authorised by law.

65 *Commonwealth Electoral Act 1918* (Cth) s 91B.

66 Ibid s 91A(2A). This provision does not apply to a Senator, member of the House of Representatives or political party.

67 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [2.2].

68 Ibid, [2.4].

8.41 Access to court records is regulated by legislation and rules of court.[69] In the Federal Court of Australia, a person is entitled to search and inspect certain documents, such as pleadings, judgments or orders, unless the court or a judicial officer has ordered that they are confidential.[70] A person who is not a party to the proceeding may only inspect certain documents, such as interrogatories or answers to interrogatories, with the leave of the court.[71] Leave will usually be granted, however, where a document has been admitted into evidence or read out in open court.[72]

8.42 A number of courts and tribunals have advised the Inquiry that they have developed internal policies and guidelines that relate to the online publication of judgments. This guidance is developed by each court and tribunal on a case-by-case basis and is directed towards the particular issues that arise from the online publication of judgments in each jurisdiction. For example, a court that deals mainly with family law matters may require different procedures about the redaction of certain personal information in judgments published online than a court that deals mainly with commercial matters.

8.43 In IP 31, the ALRC asked whether the *Privacy Act* needs to be amended in response to issues raised by the publication in electronic form of publicly available records such as public records, court records and media reports.

Submissions and consultations

Public registers

8.44 The Government of South Australia reiterated the issues associated with online publication of public registers and submitted that:

> It has often been difficult to establish the intended purpose of publicly available information if the legislation or policy that established its public nature was not specific.[73]

8.45 The Office of the Victorian Privacy Commissioner (OVPC) has issued guidelines to Victorian state agencies that collect personal information for inclusion on

---

69 See, eg, *High Court Rules 2004* (Cth) r 4.07.4; *Federal Court Rules 1979* (Cth) o 46 r 6; *Federal Magistrates Court Rules 2001* (Cth) r 2.08. In Ch 32, the ALRC discusses the partial exemption of federal courts from the operation of the *Privacy Act 1988* (Cth). In addition, the ALRC proposes that the *Privacy Act* be amended to remove the partial exemption that applies to the Australian Industrial Relations Commission, the Industrial Registrar and Deputy Industrial Registrars: Proposal 32–3. The ALRC also asks whether the *Privacy Act* should be amended to provide that federal tribunals that exercise quasi-judicial functions are exempt from some of the proposed UPPs in respect of their quasi-judicial functions: Question 32–1.

70 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).

71 Ibid o 46 r 6(3), (5).

72 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au/courtdocuments/publicdocuments.html> at 30 July 2007.

73 Government of South Australia, *Submission PR 187,* 12 February 2007.

public registers.[74] These guidelines outline circumstances where it is appropriate for an agency to give notice about online dissemination of personal information and provide 'an opportunity to suppress online dissemination of information'. The OVPC submitted that:

> There is merit in considering the introduction of public register principles or other more specific guidance for balancing the interests in privacy with the interests in favour of making records available to the public.[75]

8.46 The Law Council of Australia submitted that, in principle, if a record is available without restriction in hard copy, there should be 'no restriction upon making the record available electronically'. In circumstances where restrictions apply to access to hard copy records, however, similar restrictions should apply in the online environment.

> The restrictions that might be imposed will vary depending upon the circumstances, but could include … electronic restrictions upon downloading documents and, in other circumstances, be limited to requirements to obtain undertakings from those who access the electronic records.[76]

Court records

8.47 The OPC noted a number of issues associated with the online publication of court records. In particular, the OPC noted that the publication of such records could interfere with spent convictions laws, facilitate identity theft and lead to intimidation of those involved in court processes. The OPC, however, submitted that:

> [t]he Privacy Act is not the appropriate instrument for implementing changes to protect the personal information contained in court records … changes to court record publication are best dealt with through procedural directives or guidelines rather than through legislative intervention.[77]

8.48 The Legal Aid Commission of NSW submitted that:

> the right balance between access and disclosure of court records and judgements is not something that can be resolved by following a set of principles of general application. This is a further area where the Privacy Commissioner should be encouraged to prepare codes of practice or guidelines.[78]

Other generally available publications

8.49 One stakeholder submitted that the personal information contained in generally available publications 'promote[s] important public interests which outweigh any

---

74 Office of the Victorian Privacy Commissioner, *Public Registers and Privacy—Guidance for the Victorian Public Sector* (2004).
75 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
76 Law Council of Australia, *Submission PR 177,* 8 February 2007.
77 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
78 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

privacy issues or arguments to amend the *Privacy Act*'.[79] The National Health and Medical Research Council submitted that:

> any amendment of the *Privacy Act* to provide added protection for publicly available records should not diminish access for quality assurance and research purposes to important health information held in such records.[80]

8.50 The Legal Aid Commission of NSW noted that the 'public domain is ill-equipped to deal with the ease with which information can be made available on-line' but submitted that 'privacy does not cease to be a relevant issue just because personal information can be found on the Internet'.[81] The Office of the Information Commissioner Northern Territory submitted that, while the *Privacy Act* does not need to be amended in response to these issues,

> it is important that agencies and organisations be aware of the potential for data manipulation when considering new forms of publication made possible by new technologies.[82]

8.51 The Government of South Australia submitted that 'there is a greater risk to the proliferation of privacy abuse in the electronic environment. However, the principles of regulation remain the same'.[83] The Australian Federal Police submitted that the publication in electronic form of publicly available information does not change

> fundamentally the privacy protections that are in place for the current publication of this information as the same restrictions will apply. There is a danger to over-emphasise the ubiquitousness of internet technology and the level of interest in these records.[84]

8.52 The Australian Privacy Foundation submitted that:

> The collection, use and disclosure principles should apply to publicly available information to the maximum extent possible, preferably by reference to 'reasonable expectations' and 'public interest' tests. Despite the difficulties of enforcement, the law should challenge the entrenched idea that once personal information is in the public domain it should be available for any use.[85]

Options for reform

8.53 There are various approaches that could be taken to regulate online access to personal information contained in generally available publications. For example, some Scandinavian countries allow a substantial amount of personal information to be

---

79 Confidential, *Submission PR 165,* 1 February 2007.
80 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
81 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
82 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
83 Government of South Australia, *Submission PR 187,* 12 February 2007.
84 Australian Federal Police, *Submission PR 186,* 9 February 2007.
85 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

included in government records published on public websites.[86] At the other end of the spectrum, a Bill currently under consideration in New Zealand is intended to prevent access to births, deaths and marriages publications that were produced less than a certain number of years ago.[87]

8.54 A number of steps could be taken to protect personal information contained in generally available publications published in electronic form. Some jurisdictions have attempted to prohibit the collection of personal information contained in generally available publications. In Finland, one method to deal with the issues presented by significant amounts of online information has been to enact legislation that sets out the limited circumstances in which an employer can collect information about an employee or job applicant.[88] It may be very difficult, however, to enforce such a prohibition in the online context.

8.55 Another option is to encourage agencies and organisations to restrict the type and extent of personal information published on public websites. The type of information that is made available electronically could be limited to that which is necessary to promote the purpose of the public record.[89] Alternatively, unnecessary personal information could be removed from documents before they are published electronically. Another option is to restrict the use and disclosure of publicly available information in electronic form to that which is consistent with the public interest served by publishing the information.

ALRC's view

8.56 The ALRC agrees that the internet has changed the nature of the 'public domain'. In the ALRC's view, it is not appropriate to deal with the issues presented by the electronic publication of publicly available information by increasing the regulation of personal information held in a 'generally available publication'. There is a public interest in making certain types of information publicly available. In some circumstances, this public interest remains relevant for generally available publications published in an electronic form. In addition, it is difficult to enforce the use and disclosure of personal information in such publications. Electronic publication of generally available publications has increased, rather than decreased, these enforcement difficulties.

8.57 The ALRC notes that stakeholders' concerns about generally available publications are focused on circumstances when these publications are widely disseminated—in particular, when they are posted on the internet.

---

86 For a discussion of the significant number of Swedish government records that are published online, see E Addley, 'Sweden Tries to Lose Reputation as Snoopers' Paradise', *Guardian Unlimited Technology* (online), 19 June 2007, <technology.guardian.co.uk>.

87 See, eg, Births, Deaths, Marriages, and Relationships Registration Amendment Bill 2007 (NZ).

88 *Act on Data Protection in Working Life 2004* (Finland) s 4.

89 B Givens, *Public Records on the Internet: The Privacy Dilemma* (2002) Privacy Rights Clearinghouse <www.privacyrights.org/ar/onlinepubrecs.htm> at 31 July 2007.

8.58 As discussed above, there are inherent difficulties in regulating the use and disclosure of personal information published on the internet. Agencies and organisations should, therefore, be encouraged to restrict in the first place the type and extent of personal information that is published on the internet. In the case of public registers, the electronic publication of the register may be regulated by the legislative instrument that establishes the register—in the way that, for example, the *Commonwealth Electoral Act* regulates certain uses and disclosures of information collected from electronic versions of the electoral roll. In the ALRC's view, legislative instruments establishing public registers should set out clearly any restrictions on the use and disclosure of personal information contained on the register.

8.59 The ALRC notes that courts that publish judgments in the online environment have developed internal policies and guidelines that deal with particular issues that arise in the relevant jurisdiction. The ALRC also notes that SCAG is considering the issue of online publication of criminal records. In addition, the OPC should provide education and guidance to agencies and organisations directed towards restricting the type and extent of personal information that is published online. The ALRC notes that the OPC has issued an Information Sheet (Information Sheet 17) that focuses on the collection by organisations of personal information contained in generally available publications.[90] Information Sheet 17 also lists some tips for good privacy practice that apply to agencies and organisations required by law to make personal information publicly available.

8.60 This information sheet could be used as the basis for providing more detailed guidance to agencies and organisations that make personal information about individuals available in the online environment. The guidance should apply whether or not the agency or organisation is required by law to make the personal information publicly available. The guidance could provide detailed advice on issues outlined in Information Sheet 17—for example, factors that agencies and organisations should consider before publishing personal information in an electronic form, such as whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual.

8.61 The proposed guidance should also set out clearly the requirements with which both agencies and organisations must comply when collecting information from generally available publications for inclusion in a record (or another generally available publication). The ALRC notes that the definition of a 'record' includes a 'database'.[91] It is highly unlikely that personal information collected from generally available publications—for example, by an organisation for the purposes of direct marketing or data-matching—will *not* be included in some form of record (or another

90 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003).

91 *Privacy Act 1988* (Cth) s 6(1). The definition of a 'record' is discussed further in Ch 3.

generally available publication).[92] The proposed guidance should set out the steps that should be taken by an agency or organisation that collects personal information from generally available publications to meet the obligations in the proposed 'Collection', 'Specific Notification', 'Data Quality' and 'Direct Marketing' principles.[93]

8.62 Finally, the ALRC notes that both the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) regulate personal information that is collected for inclusion in a record or generally available publication, but the principles only apply to personal information that is held in a record. The way that this is achieved in the legislation, however, differs. IPPs 1, 2 and 3 refer to both a 'record' and a 'generally available publication' but IPPs 4–11 refer only to a 'record'. In relation to the NPPs, the application of the relevant principles to records and generally available publications is set out in s 16B. The ALRC's view is that the latter approach is preferable and notes that it will be necessary to make a consequential amendment to s 16B of the *Privacy Act* if the proposed Unified Privacy Principles are implemented.[94]

Proposal 8–1 The Office of the Privacy Commissioner should provide guidance that relates to generally available publications in an electronic form. This guidance should:

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out certain factors that agencies and organisations should consider before publishing personal information in an electronic form (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

(c) set out the requirements in the proposed Unified Privacy Principles with which agencies and organisations need to comply when collecting personal information from generally available publications for inclusion in a record or another generally available publication (for example, when a reasonable person would expect to be notified of the fact and circumstances of collection).

92 In Ch 6, the ALRC proposes that the OPC issue guidance on data-matching to organisations: Proposal 7–6.

93 The proposed 'Collection', 'Specific Notification' and 'Data Quality' principles apply to both agencies and organisations. The proposed 'Direct Marketing' principle only applies to organisations.

94 The proposed Unified Privacy Principles are discussed in Part D.

9. Identity Theft

Contents

Introduction 393
What is identity theft? 394
How prevalent is it? 395
Criminalising identity theft 396
- Federal legislation 396
- State and territory legislation 397
- Other jurisdictions 398

Other responses to identity theft 398
Identity theft and privacy laws 399
- The Unified Privacy Principles 399
- Breach notification 399
- Publicly available information in electronic form 400
- Unique multi-purpose identifiers 400
- Credit reporting 401

Introduction

9.1 This chapter discusses identity theft and privacy. It commences by defining identity theft and discussing existing responses to it in Australia and overseas. It then provides an overview of the ways in which privacy laws can assist in preventing identity theft and minimising the harm caused by it after it has occurred. Specific options for reform of privacy laws that may help to address the problem of identity theft are discussed in further detail throughout this Discussion Paper.

9.2 Identity theft has existed for centuries. It has been argued, however, that it is becoming more prevalent in today's society because of developments in technology.[1] For instance, developments in information and communications technology mean that agencies and organisations now store vast amounts of identifying information electronically. Any breach of the secure storage of this information can increase the risk of identity theft for the people to whom the stored identifying information relates. Further, electronic commerce and electronic government create impersonal transacting environments that are conducive to identity crime, and developments in computer

1 See, eg, N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 1; R Lozusic, *Fraud and Identity Theft: Briefing Paper 8/2003* (2003) Parliament of New South Wales—Parliamentary Library.

technology have greatly increased the ability of individuals to forge identifying documents.[2]

What is identity theft?

9.3 While there is widespread concern about identity theft and its impact on privacy, there is little consensus about the definition of the term 'identity theft'. Commentators, legislators and policy makers tend to use the terms 'identity crime', 'identity fraud' and 'identity theft' in differing ways and, at times, interchangeably.

9.4 In this Discussion Paper, 'identity crime' is used broadly to describe any offence committed using a fabricated, manipulated or stolen identity.[3] 'Identity fraud' is used to describe a type of identity crime—namely, the gaining of a benefit (or the avoidance of an obligation) through the use of a fabricated, manipulated or stolen identity. 'Identity theft' is used to describe the illicit assumption of a pre-existing identity of a living or deceased person, or of an artificial legal entity such as a corporation.[4]

9.5 Identity theft can be committed for a number of reasons. For example, as noted above, the assumption of another person's identity can facilitate the commission of identity crimes, including identity fraud, people smuggling and terrorism offences.[5] It can also enable a person to avoid detection in order to avoid meeting obligations, such as making child support payments. Alternatively, identity theft may be committed simply to distress or intimidate the person to whom the illicitly acquired identity information relates.[6]

9.6 There are many ways in which identifying information about another person can be surreptitiously acquired, including through the theft of a person's mail, wallet, purse or handbag, or through the retrieval of documents from a person's rubbish. The identifying information of another person can also be acquired through more sophisticated means, such as skimming the person's credit card or hacking into an electronic database containing identifying information about the person.[7] 'Phishing' is another method that is used to acquire information in the online environment. Phishing typically refers to the practice where an email purporting to be from a trusted entity directs a recipient to a website that closely resembles the website of that entity. The

---

2 See, eg, S Cuganesan and D Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (2003) Securities Industry Research Centre of Asia-Pacific, 1.

3 Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006), 15.

4 Ibid, 15.

5 Australasian Centre for Policing Research, *Australasian Identity Crime Policing Strategy 2006–2008 of the Australasian and South West Pacific Region Police Commissioners' Conference* (2005), 1.

6 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Discussion Paper, Model Criminal Code Chapter 3, Credit Card Skimming Offences* (2004), 31.

7 N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 5–6.

'phisher' can then acquire any information the person enters on the 'fake' website, such as the person's name or online banking password.[8]

9.7 Identity theft can be a traumatic experience for the person whose identifying information is 'stolen'. A victim of identity theft may suffer direct financial loss as a result of the theft. In addition, he or she may incur costs when attempting to prevent the continued use of his or her identifying information. Further, a victim of identity theft is typically required to expend a large amount of time and effort countering the adverse effects of the theft. For example, he or she may be required to restore his or her credit rating, or correct errors in his or her criminal history.[9]

How prevalent is it?

9.8 There is very little information about the prevalence of identity theft in Australia. This is partly because it is not generally a criminal offence. Rather, it is the later use of the information for certain purposes that attracts criminal liability. This makes it difficult to locate information about rates of identity theft. In addition, not all instances of identity theft are reported to authorities or otherwise disclosed. Agencies and organisations in particular may be reluctant to report identity theft for fear that it will cause reputational damage or expose weaknesses in their security systems.[10]

9.9 In 2000, the House of Representatives Standing Committee on Economics, Finance and Public Administration recommended that Australian governments and industries work together to develop national statistics on the extent and cost of identity fraud.[11] In response to this recommendation, the Australian Transaction Reports and Analysis Centre's Steering Committee on Proof of Identity commissioned a report on the nature, cost and extent of identity fraud in Australia. This report found that the cost of identity fraud to Australia in 2001–02 was approximately $1.1 billion.[12] This estimate included the costs associated with preventing, detecting and responding to identity fraud, as well as losses directly incurred as a result of the fraud.[13] Unfortunately, given its focus on *identity fraud*, which includes fraud committed using fictitious identity information, this report does little to illuminate the extent or cost of *identity theft* in Australia.

---

8 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Discussion Paper—Identity Crime* (2007), 5.

9 See J Blindell, *Review of the Legal Status and Rights of Victims of Identity Theft in Australasia* (2006) Australasian Centre for Policing Research, 5.

10 N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 3.

11 Parliament of Australia—House of Representatives Standing Committee on Economics Finance and Public Administration, *Numbers on the Run—Review of the ANAO Report No 37 1998–99 on the Management of Tax File Numbers* (2000), rec 18.

12 S Cuganesan and D Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (2003) Securities Industry Research Centre of Asia-Pacific, 55.

13 Ibid, Ch 5.

9.10 In 2003, the Australian Institute of Criminology and PricewaterhouseCoopers released the results of a study of 155 serious fraud prosecutions completed in Australia and New Zealand in 1998 and 1999.[14] Stolen identities were used in approximately 13% of the cases studied.[15]

Criminalising identity theft

Federal legislation

9.11 Identity theft is not a federal offence in Australia. There are, however, numerous federal offence provisions that can be used to prosecute offenders who use illicitly acquired personal information when engaging in certain activities. These include offence provisions in the *Criminal Code* (Cth),[16] as well as in other pieces of federal legislation, such as the *Financial Transaction Reports Act 1988* (Cth)[17] and the *Migration Act 1958* (Cth).[18]

9.12 In 2000, the House of Representatives Standing Committee on Legal and Constitutional Affairs concluded that the offences to be inserted into the *Criminal Code* (Cth) by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 1999* (Cth) dealt adequately with criminal conduct related to identity fraud.[19]

9.13 Nevertheless, in 2004 a new part containing 'financial information offences' was inserted into Chapter 10 of the *Criminal Code*.[20] Accordingly, it is now a federal offence dishonestly to obtain or deal in personal financial information without the consent of the person to whom the information relates.[21] The definition of 'personal financial information' is broad and includes all information relating to a person that may be used, alone or in conjunction with other information, to access funds, credit or other financial benefits.[22]

9.14 The financial information offences in the *Criminal Code* were intended to address credit card skimming—the illicit capturing or copying of legitimate credit card

---

14 Australian Institute of Criminology and PricewaterhouseCoopers, *Serious Fraud in Australia and New Zealand*, Australian Institute of Criminology Research and Public Policy Series No 48 (2003).

15 Ibid, 2.

16 See, eg, *Criminal Code* (Cth) ss 134.1 (obtaining property by deception), 134.2 (obtaining a financial advantage by deception), 135.1 (general dishonesty), 135.2 (obtaining financial advantage), 135.4 (conspiracy to defraud).

17 See, eg, *Financial Transaction Reports Act 1988* (Cth) s 24 (opening account, etc in false name).

18 See, eg, *Migration Act 1958* (Cth) s 234 (false papers etc).

19 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999* (2000), [3.8]–[3.10].

20 *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2) 2004* (Cth) sch 3.

21 *Criminal Code* (Cth) s 480.4.

22 Ibid s 480.1(1).

data[23]—and internet banking fraud.[24] They appear, however, to be broad enough to cover many instances of identity theft.

9.15 In April 2007, the Model Criminal Law Officers' Committee released a Discussion Paper on identity crime.[25] Using the broad term 'identity crime' to refer to practices including identity theft and identity fraud, the Committee recommended the creation of three identity crime model offences. It recommended a general identity crime offence of capturing, using or transferring another person's personal information with the intention of committing an indictable or serious offence. The Committee also recommended two specific offences that would prohibit, in certain circumstances, a person from providing to a third person the identification information of another person, or possessing equipment that could be used to create identification information.[26] At the time of writing in July 2007, the Committee is conducting consultations in preparation for its final report, which is to be published later in 2007.

State and territory legislation

9.16 It is not an offence to assume or adopt another person's identity in the majority of Australian states and territories. There are, however, numerous state and territory offences that can be used to prosecute offenders who use illicitly obtained identity information to commit criminal offences.[27]

9.17 In some circumstances, however, identity theft is a criminal offence in South Australia. Section 144B of the *Criminal Law Consolidation Act 1935* (SA) makes it an offence to assume the identity of another person (whether living or dead, real or fictional, natural or corporate) with the intent to commit or facilitate the commission of a 'serious criminal offence'.[28] Section 144C makes it an offence to use the 'personal identifying information' of a living or deceased person, or a body corporate, with the intent to commit or facilitate the commission of a serious criminal offence. In March 2007, similar offence provisions were enacted in Queensland.[29]

---

23 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Discussion Paper, Model Criminal Code Chapter 3, Credit Card Skimming Offences* (2004), 1.

24 Commonwealth, *Parliamentary Debates*, House of Representatives, 4 August 2004, 32035 (P Slipper), 32036–32037.

25 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Discussion Paper—Identity Crime* (2007).

26 Ibid, 24–30.

27 See R Smith, 'Examining the Legislative and Regulatory Controls on Identity Fraud in Australia' (Paper presented at Marcus Evans Conferences, Corporate Fraud Strategy: Assessing the Emergency of Identity Fraud, Sydney, 25–26 July 2002).

28 A 'serious criminal offence' is an indictable offence or an offence prescribed by regulation: see *Criminal Law Consolidation Act 1935* (SA) s 144A.

29 The *Criminal Code and Civil Liability Amendment Act 2007* (Qld) s 6 inserts a new section into the *Criminal Code Act 1899* (Qld), which in certain circumstances makes it an offence to obtain or deal with identification information: *Criminal Code Act 1899* (Qld) s 408D.

Other jurisdictions

9.18 In October 1998, the United States Congress passed the *Identity Theft and Assumption Deterrence Act of 1998*. This Act made it a federal offence, punishable by up to 15 years imprisonment or a fine of US$250,000, to

> knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law'.[30]

9.19 The *Identity Theft Penalty Enhancement Act of 2004* (US) established penalties for the offence of aggravated identity theft. Identity theft is also an offence in the vast majority of states in the United States.[31]

9.20 In the United Kingdom it is also an offence, with some exceptions, to obtain, disclose or procure the disclosure of personal data without the consent of the data controller.[32] This offence provision could be used to prosecute those who engage in identity theft. The *Identity Cards Act 2006* (UK) makes it an offence to possess or control false identity documents, including genuine documents that belong to another person.[33]

Other responses to identity theft

9.21 It has been argued that criminalising identity theft may be ineffective because it is difficult to detect[34] and prosecute successfully.[35] Other responses to identity theft can be divided into responses aimed at preventing identity theft and responses aimed at remedying its adverse effects after it has occurred.

9.22 Initiatives aimed at preventing identity theft generally aim to:

- educate individuals about how to minimise the risk of identity theft;
- enhance the security features of identification documents so that they cannot be altered or forged; and

---

30 *Identity Theft and Assumption Deterrence Act of 1998* 18 USC § 1028 (US).

31 United States Government Federal Trade Commission, *State Laws: Criminal* <www.ftc.gov> at 30 July 2007.

32 *Data Protection Act 1998* (UK) s 55.

33 *Identity Cards Act 2006* c 15 (UK) s 25.

34 D Solove, 'The Legal Construction of Identity Theft' (Paper presented at Symposium: Digital Cops in a Virtual Environment, Yale Law School, New Haven, 26–28 March 2004).

35 Ibid; N Dixon, *Identity Fraud: Research Brief No 2005/03* (2005) Parliament of Queensland—Parliamentary Library, 10.

- strengthen the procedures used to authenticate the identity of individuals engaging in transactions with agencies or organisations.[36]

9.23 Initiatives aimed at minimising the harm of identity theft tend to focus on assisting victims of identity theft to remedy the adverse effects of the theft and to regain control over the use and disclosure of their personal information.

Identity theft and privacy laws

9.24 Identity theft represents a threat to privacy when it involves the theft or assumption of the identity of a living person. Privacy laws can assist in preventing identity theft and minimising the harm caused by it after it has occurred.

The Unified Privacy Principles

9.25 A number of the privacy principles in the *Privacy Act 1988* (Cth) are relevant to the problem of identity theft. Some of these principles, such as those requiring personal information to be stored securely and those restricting the circumstances in which personal information can be disclosed, may assist in preventing identity theft by preventing the widespread dissemination of personal information. Others, such as the principles requiring personal information contained in a record to be accurate, may assist in minimising the harm caused by identity theft after it has occurred. The privacy principles are discussed in detail in Part D.

Breach notification

9.26 It has been argued that one way of combating identity theft is to require agencies and organisations to notify individuals of any unintended or unauthorised disclosure of their personal information. This alerts individuals to the possibility that they may be at risk of identity theft and may assist them to prevent the theft of their personal information. Alternatively, it may assist them to detect promptly any theft of their personal information. In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether agencies or organisations should be required to advise individuals of any misuse, loss or unauthorised access, modification or disclosure of personal information.[37] The question whether the *Privacy Act* should contain a breach notification requirement is discussed in Chapter 47. The ALRC proposes that the *Privacy Act* be amended to include a Part on data breach notification, which would

---

36 For example, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), and the rules issued under s 229 of the Act, describe the customer identity verification procedures that must be followed by a reporting entity that delivers to a customer a service that is designated by the Act. See, eg, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) pts 2, 7 and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1) 2007* (Cth) chs 4, 6–7.

37 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–35 and 11–3.

require an agency or organisation to notify the OPC and affected individuals of a data breach in certain circumstances.[38]

Publicly available information in electronic form

9.27 Information stored in electronic form can be easily accessed, searched and aggregated. This is particularly so when it is available online. Online public records often contain a wealth of identifying information and there is concern that this information may be used to facilitate identity theft.[39] In IP 31, the ALRC asked whether the *Privacy Act* needed to be amended in response to issues raised by the publication in electronic form of publicly available records.[40] This issue is discussed in Chapter 8. A discussion of security in the online environment is contained in Chapter 6. The ALRC proposes that the OPC should provide guidance on generally available publications available in an electronic form.[41]

9.28 The ALRC also asks in Chapter 8 whether the online content regulation scheme set out in the *Broadcasting Services Act 1992* (Cth), and in particular the ability to issue take-down notices, should be expanded beyond the *National Classification Code* and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy. If so, the ALRC is interested in hearing views on the criteria that should be used to determine when a take-down notice should be issued, and the appropriate body to issue the take-down notice.[42]

Unique multi-purpose identifiers

9.29 The use of unique multi-purpose identifiers enhances the ability of agencies and organisations to compile and aggregate large amounts of personal information about individuals. For example, it has been noted that the most valuable piece of identifying information for identity thieves in the United States is the Social Security Number. Social Security Numbers are the key to assuming another person's identity because 'they are used to match consumers with their credit histories and many government benefits'.[43] In IP 31, the ALRC asked what role (if any) the *Privacy Act* should play in regulating the use of unique multi-purpose identifiers.[44] In Chapter 27, the ALRC proposes that, before an agency introduces any unique multi-purpose identifier, the Australian Government should consider, in consultation with the Privacy Commissioner, the need for a privacy impact assessment.[45]

---

38 Proposal 47–1.
39 See, eg, L Myers, 'Online Public Records Facilitate ID Theft', *MSNBC* (online), 5 February 2007, <www.msnbc.msn.com>.
40 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 11–5.
41 Proposal 8–1.
42 Question 8–1.
43 President's Identity Theft Task Force, *Interim Recommendations* (2006), 2.
44 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 12–3.
45 Proposal 27–5.

Credit reporting

9.30 In Issues Paper 32, *Review of Privacy: Credit Reporting Provisions* (IP 32), the ALRC asked whether the credit reporting provisions of the *Privacy Act* should be amended to provide expressly for the problem of identity theft.[46] In the United States, the *Fair Credit Reporting Act 1970* (US) contains provisions designed to assist victims of identity theft. For example, this Act enables a victim of identity theft to require that a credit reporting agency insert a 'fraud alert' on a credit information file.[47] Further, in some parts of the United States, victims of identity theft can request a 'freeze' on their credit information files.[48] These and other ways in which the credit reporting provisions of the *Privacy Act* can address the problem of identity theft are discussed in Chapter 52. The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.[49]

9.31 In IP 32, the ALRC also noted that children and young people are a common target for identity theft as they often have unblemished or non-existent credit records.[50] The ALRC asked how the collection, use and disclosure of personal information relating to children and young people in credit information files and credit reports should be regulated.[51] This issue is also discussed in Chapter 52. The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals the credit provider or credit reporting agency knows to be under the age of 18 years.[52]

---

46 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–23.

47 A fraud alert is a statement that notifies prospective users of a credit report that the individual to whom it relates 'may be a victim of fraud, including identity theft': *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) § 1681c–1.

48 See, eg, *California Civil Code* § 1785.11.2–1785.11.6. Placing a freeze on a credit information file prevents it from being accessed by potential creditors.

49 Proposal 52–1.

50 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.147].

51 Ibid, Question 5–24.

52 Proposal 52–8.

10. Overview—Interaction, Inconsistency and Fragmentation

Contents

Introduction 405
The costs of inconsistency and fragmentation 406
- Sharing information 406
- Compliance burden and cost 407
- Multiple regulators 407
- Government contractors 408

Federal information laws 408
- Terms and definitions 409
- *Freedom of Information Act 1982* (Cth) 409
- *Archives Act 1983* (Cth) 410
- A single information Act? 410
- A single regulator? 411
- Secrecy provisions 411
- Obligations of confidence 411

Required or authorised by or under law 412
- The meaning of 'required or authorised by or under law' 412
- *Census and Statistics Act 1905* (Cth) 412
- *Corporations Act 2001* (Cth) 413
- *Commonwealth Electoral Act 1918* (Cth) 413
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* 414

Interaction with state and territory laws 415
- Federal, state and territory regimes that regulate personal information 415
- Privacy rules, codes and guidelines 416
- Residential tenancy databases 416

Introduction

10.1 Part C considers how the *Privacy Act 1988* (Cth) interacts with other federal, state and territory laws, and identifies areas of fragmentation and inconsistency in the regulation of personal information. A number of issues related to inconsistency and fragmentation are considered in other Parts of the Discussion Paper. For instance, the inconsistencies between the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) are considered in Part D, the fragmentation that results from the various exemptions under the *Privacy Act* is outlined in Part E, inconsistency and

fragmentation in the regulation of health information is discussed in Part H, and the interaction of the *Privacy Act* and telecommunications legislation is considered in Part J.

The costs of inconsistency and fragmentation

10.2 Chapter 11 discusses some specific problems caused by inconsistency and fragmentation. These problems include impediments to information sharing, unjustified compliance burden, multiple privacy regulators and issues related to government contractors. The ALRC makes a number of proposals throughout this Discussion Paper directed to dealing with problems caused by inconsistency and fragmentation in privacy regulation. Perhaps the most significant of these proposals is the adoption of the Unified Privacy Principles (UPPs) at the federal, state and territory level.[1] The ALRC's view is that these proposals will deal with many of the problems identified in Chapter 11.

Sharing information

10.3 Inconsistent, fragmented and multi-layered privacy regulation can contribute to confusion about how to achieve compliance with privacy regulation and therefore a hesitance by organisations and agencies to share information.

10.4 In submissions to the Inquiry, a wide range of examples were provided where inconsistent, fragmented and multi-layered privacy laws have prevented or impeded information sharing. For example, the ALRC heard numerous examples of agencies and organisations using 'because of the *Privacy Act*' as an excuse for not providing information. Submissions also noted that inconsistent, fragmented and multi-layered privacy laws can act as a barrier to information sharing between federal, state and territory government agencies. This was identified as a particular issue in the areas of child protection, service provision to vulnerable persons, law enforcement and medical research.

10.5 The ALRC's view is that it is undesirable that inconsistency and fragmentation in privacy laws prevent appropriate information sharing. The ALRC therefore makes a number of proposals that are directed at encouraging agencies and organisations to design information-sharing schemes that are compliant with privacy requirements or, where necessary, seek suitable exemptions or changes to legislation to facilitate information-sharing projects. These proposals include the Office of the Privacy Commissioner (OPC) providing further guidance to agencies and organisations on privacy requirements affecting information sharing, and the establishment of an inter-agency working group to identify opportunities where it would be appropriate to share personal information among Australian Government agencies.

---

1 Proposal 4–4.

10.6 A number of the ALRC's proposals are directed at achieving greater transparency in information sharing arrangements. The ALRC proposes that agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information, and the development and publication of a framework relating to cross-border sharing of personal information within Australia by intelligence and law enforcement agencies.

Compliance burden and cost

10.7 The Terms of Reference for this Inquiry require the ALRC to consider 'the desirability of minimising the regulatory burden on business'. The ALRC received a large number of submissions that claimed that the proliferation and fragmentation of privacy laws have increased compliance burden and cost for both agencies and organisations. Others submitted, however, that there is little evidence of the existence or extent of any unwarranted compliance burden.

10.8 It was noted in submissions that inconsistency and fragmentation in privacy regulation are particularly problematic for organisations that operate in more than one Australian jurisdiction, and complicate the implementation of programs and services at a national level. While stakeholders focused on the financial costs of this complexity, costs can also include social costs, such as delays in the provision of health services.

10.9 The ALRC considers that the compliance burden caused by the *Privacy Act* is justified. Inconsistency and fragmentation in the regulation of personal information at the federal, state and territory level, however, create an unjustified additional compliance burden. The ALRC's proposals for reform, including those highlighted in this chapter, would help reduce compliance costs, including through the adoption of a single set of privacy principles at the federal, state and territory level and a redraft of the *Privacy Act* to minimise its complexity.

Multiple regulators

10.10 Some industries are required to comply with multiple layers of privacy regulation, which are overseen by more than one regulator. In submissions to the Inquiry, it was noted that the lack of consistency of federal and state and territory privacy regimes leads to confusion about where and how to complain in relation to a privacy matter. Other submissions identified advantages in having multiple privacy regulators.

10.11 The ALRC considers that it is preferable to have privacy regulators at the federal, state and territory level. This ensures that people in each jurisdiction have a regulator they can approach for advice and to make a complaint, and agencies and organisations have access to a regulator who is aware of their local circumstances and

can provide advice and training on implementing the legislation. Further, industry-specific regulators provide industry expertise that the OPC cannot provide.

10.12 There is evidence to suggest that multiple privacy regulators can create problems for individuals, agencies and organisations. In Chapters 45 and 64, the ALRC makes a number of proposals aimed at improving the operation of multiple privacy regulators. These proposals include: amending the *Privacy Act* to empower the Privacy Commissioner to delegate all or any of his or her complaint-handling powers; the development of memoranda of understanding between the OPC and other bodies with responsibility for privacy; and the development and publication of complaint-handling policies, enforcement guidelines and educational material that address the role and functions of the various bodies with responsibility for information privacy.

Government contractors

10.13 The *Privacy Act* imposes obligations on agencies entering into contracts to provide services to or on behalf of the agency. The Act requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider or a subcontractor does not do an act or engage in a practice that would breach the IPPs.

10.14 Stakeholders submitted that these provisions remain appropriate and effective. An outstanding issue, however, is whether the definitions of 'contracted service provider' and 'state contract' under the *Privacy Act* are adequate, and whether they cover all the types of activities that organisations might perform on behalf of agencies. The ALRC is interested in views on this issue.

10.15 Some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state privacy principles for the purposes of the contract. Other state regimes provide that compliance with the state privacy regime is subject to outsourcing arrangements, or are silent on this issue.

10.16 There are concerns that state or territory government contractors, who are otherwise private sector organisations, may not be bound by the *Privacy Act* or equivalent standards when performing functions under state or territory contracts. In Chapter 11, the ALRC considers whether the *Privacy Act* should be amended to include a 'roll-back provision' to cover state contractors. In the ALRC's view, however, such a law would intrude too heavily on state and territory government business. Instead, the ALRC proposes that state and territory privacy legislation should include provisions relating to state and territory contractors.

Federal information laws

10.17 Chapter 12 considers how the *Privacy Act 1988* (Cth) interacts with a number of federal laws that regulate the handling of personal information.

Terms and definitions

10.18 Federal legislation other than the *Privacy Act* regulates the handling of personal information. Sometimes this legislation adopts different terms or definitions to those used in the *Privacy Act*. For example, the concept of 'personal information' is central to the regime established by the *Privacy Act*, but other federal legislation adopts different terms such as 'personal affairs' to describe similar information. The definitions of other terms used in the *Privacy Act* also sometimes differ from the same terms in other federal legislation.

10.19 In the ALRC's view, the inconsistent use of terms and definitions in privacy legislation contributes to the complexity of privacy law and may increase compliance burden and cost. The ALRC therefore proposes that the Australian Government should ensure the consistency of definitions and key terms in federal legislation that regulates the handling of personal information. The ALRC acknowledges that there will be occasions, however, when other policy considerations will justify the use of terms or definitions that differ from those used in the *Privacy Act*.

Freedom of Information Act 1982 (Cth)

10.20 The interrelationship between the *Freedom of Information Act 1982* (Cth) (FOI Act) and the *Privacy Act* is significant. The FOI Act and the *Privacy Act* both regulate the way in which information is handled in government, but the Acts have different objectives. Freedom of information legislation is mainly concerned with transparency in government and protects privacy only to the extent that non-disclosure is, on balance, in the public interest. In contrast, privacy legislation is focused primarily on data protection and provides for transparency only to the extent that it enhances the information privacy rights of individuals.

Disclosure of personal information

10.21 The FOI Act provides that every person has a legally enforceable right to obtain access to a document of an agency or an official document of a minister, other than an exempt document. Section 41(1) of the FOI Act provides that a document is an exempt document if its disclosure under the Act would involve the unreasonable disclosure of personal information about any person (including a deceased person). In the ALRC's view, the relationship between the FOI Act and the *Privacy Act* requires clarification. The proposed 'Use and Disclosure' principle sets out the appropriate test for when a disclosure of personal information will be reasonable.

Access and correction

10.22 Both the FOI Act and the IPPs enable individuals to access personal information about them and to amend or annotate that information if it is incorrect, incomplete, out-of-date or misleading. The rights provided by the *Privacy Act* are found in IPP 6 and IPP 7. The amendment rights in the FOI Act are located in Part V and are dependent on

a person having previously obtained lawful access under the Act to the relevant documents. A number of stakeholders submitted that the overlap has created confusion for both agencies and the public.

10.23 In Chapter 12, the ALRC considers various models for dealing with the overlap, and proposes that an individual's right to access or correct his or her own personal information held by an agency should be dealt with under a new Part in the *Privacy Act*. The proposed Part dealing with access and correction of personal information held by agencies retains the same requirements as IPP 6 and IPP 7 and sets out a simplified process for an individual to access and correct personal information about him or her, held by an agency.

Archives Act 1983 (Cth)

10.24 The *Archives Act 1983* (Cth) establishes the National Archives of Australia and provides for the preservation of the archival resources of the Commonwealth. It also creates an access regime whereby the public generally has a right of access to Commonwealth records that are more than 30 years old. The *Archives Act* provides some protection of information relating to the 'personal affairs' of any person, including a deceased person.

10.25 One submission to the Inquiry suggested that amending the 'personal affairs' exemption to apply to 'personal information' would protect privacy better, and harmonise the *Archives Act* with both the *Privacy Act* and the FOI Act.[2] There was strong opposition to this amendment from other stakeholders. It was noted that the reference to 'personal affairs' in the exemption is an appropriate recognition of the different age and sensitivity of the information covered by the Act, that such an amendment would needlessly restrict access to records, and would increase the workload of officers making access decisions under the Act. The ALRC concludes that, in the absence of any identifiable problem in this area, the benefits in changing the exemption to refer to 'personal information' do not outweigh the disadvantages of such an amendment.

A single information Act?

10.26 One option for consideration is whether, given the significant overlap between the FOI Act and the *Privacy Act*, the two Acts should be consolidated into a single Act. A number of overseas jurisdictions have combined freedom of information and privacy legislation. Another option would be to consolidate the FOI Act, the *Privacy Act* and the *Archives Act* into a single Act. An example of such legislation is the *Information Act 2002* (NT).

10.27 There was little support among stakeholders for combining the *Privacy Act*, FOI Act and *Archives Act*. Stakeholders noted that the three Acts have different purposes,

---

2 'Personal affairs' is generally considered to be a narrower concept than 'personal information'.

and that the ALRC should focus on the harmonisation of the Acts. In the ALRC's view, there is insufficient benefit in combining the Acts to outweigh the disadvantage in disturbing the current legislative framework.

A single regulator?

10.28 The ALRC has also considered the option of the same body administering the *Privacy Act* and the FOI Act. This is the case in the Northern Territory, and a number of overseas jurisdictions, for example, the Office of the Information and Privacy Commissioner for British Columbia, the Office of the Ontario Information and Privacy Commissioner, and the United Kingdom Information Commissioner's Office.

10.29 There was little support for this proposal. It was noted in submissions that the *Privacy Act* and the FOI Act have different focuses, and should be administered by two different bodies. Further, a number of stakeholders supported a separate body, such as a Freedom of Information Commissioner, to oversee freedom of information at the federal level.

10.30 The ALRC does not propose the establishment of a single body to administer the *Privacy Act* and the FOI Act. In the ALRC's view, however, the Australian Government should establish a statutory office of the FOI Commissioner to oversee the administration of the FOI Act and these functions should be conferred on the Commonwealth Ombudsman.

Secrecy provisions

10.31 Federal legislation contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Secrecy provisions usually are based on the need to preserve the secrecy of government operations in order for government to function effectively. In *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act,* rather than secrecy provisions in specific statutes, should regulate the disclosure of personal information by Australian Government agencies.

10.32 There was no support for having the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by agencies. The ALRC considers that it is appropriate that specific statutes include secrecy provisions designed to protect information, because secrecy provisions do not relate solely to personal information; but also protect other information, for example, commercial information, security details and operational information.

Obligations of confidence

10.33 Part VIII of the *Privacy Act* was introduced to remedy the law of confidence in a number of respects, including to extend the right to enforce a duty to preserve confidentiality in respect of personal information to the subject of the information. In

IP 31, the ALRC asked whether the provisions in Part VIII of the *Privacy Act* are necessary, and whether the provisions are adequate and should be contained in the *Privacy Act* or elsewhere. The provisions have never been used. The ALRC proposes that the confidentiality provisions contained in Part VIII of the *Privacy Act* be repealed.

Required or authorised by or under law

10.34 Chapter 13 considers the meaning of the phrase 'required or authorised by or under law', and outlines a new exception for acts and practices that are '*specifically* authorised by or under law'. The chapter then considers a number of federal Acts that require or authorise acts and practices for the purposes of the *Privacy Act*. These laws include the *Census and Statistics Act 1905* (Cth), the *Corporations Act 2001* (Cth), the *Commonwealth Electoral Act 1918* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth). The interaction between these laws and the *Privacy Act* has been the subject of recent public debate.

The meaning of 'required or authorised by or under law'

10.35 An act or practice required or authorised by or under law is an exception (the 'required or authorised exception') to a number of the IPPs and the NPPs. The ALRC proposes that acts or practices that are required or authorised by or under law should be an exception to a number of the proposed UPPs.

10.36 In the ALRC's view, there is a public expectation that governments are able to make laws to facilitate the handling of information in certain appropriate and necessary ways. The required or authorised exception reflects this expectation. The ALRC has, however, identified two areas where an exception in relation to acts and practices that are 'specifically authorised' by or under law would be beneficial. An exception for acts and practices that are 'specifically authorised' would require the law expressly to authorise a defined class of acts and practices.

10.37 The scope of the required or authorised exception, however, requires clarification. Submissions noted that the ambiguity in the operation of this exception can create uncertainty for individuals, agencies, organisations and privacy regulators. The ALRC discusses various methods to clarify the scope of the exception, including clear references to the required or authorised exception in legislative provisions that intend to rely on the exception. The ALRC also considers the development and publication of a list of provisions in other legislation that requires or authorises certain acts or practices that would otherwise be regulated by the *Privacy Act*. This proposal raises a range of issues, including whether the list should have the force of law, whether it should be comprehensive or indicative and who should compile and maintain it.

Census and Statistics Act 1905 (Cth)

10.38 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).

The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, industry, businesses and private individuals.

10.39 Submissions raised a number of issues concerning two recent developments in relation to the census—the retention of name-identified information collected in the census for 99 years, and a proposal to enhance the value of the census by combining it with future censuses and possibly other datasets held by the ABS. The ALRC does not make a proposal in relation to these developments. In the ALRC's view, the *Privacy Act* and the *Census and Statistics Act* continue to provide adequate protection of personal information collected as part of the census.

Corporations Act 2001 (Cth)

10.40 Section 168 of the *Corporations Act 2001* (Cth) requires companies and registered schemes to maintain a register of members, and if relevant, a register of option holders and a register of debenture holders. The *Corporations Act* also requires companies to allow anyone to inspect these registers.

10.41 A number of issues were raised in submissions in relation to registers of members. The ALRC does not, however, make any proposals concerning the availability of registers of members. The ALRC notes the significant public interest in disclosure of who has control or an interest in a company. Further, the *Corporations Act*, and regulations made under it, provide significant protection of personal information held on a register of members.

Commonwealth Electoral Act 1918 (Cth)

10.42 Part VI of the *Commonwealth Electoral Act 1918* (Cth) provides for the establishment of an electoral roll. It is compulsory for all eligible persons in Australia to maintain continuous enrolment on the Commonwealth electoral roll for the purposes of federal elections and referendums. The names and addresses of all electors on the Commonwealth electoral roll are available for public inspection in various formats specified under the *Commonwealth Electoral Act*.

10.43 A range of issues raised in submissions related to the handling of personal information held on the electoral roll. In particular, the ALRC heard concerns about the use of old electoral rolls for unauthorised purposes, such as direct marketing. The ALRC proposes that, if the exemption under the *Privacy Act* that applies to registered political parties and political acts and practices is not removed, the *Commonwealth Electoral Act* should be amended. This amendment should provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information in relation to the electoral roll and certified lists of voters, must take reasonable steps to protect the information from misuse and loss and

from unauthorised access, modification or disclosure; and destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.

10.44 The ALRC also proposes that the Australian Electoral Commission and state and territory electoral commissions, in consultation with the OPC, develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purpose of the continuous update of the electoral roll.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

10.45 The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) is intended to enable individual businesses to minimise money laundering and terrorism financing risks. The Act sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person who provides 'designated services'. A large number of 'designated services' are listed in the Act, including opening an account, making a loan, and supplying goods by way of hire purchase.

10.46 The Act requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer. In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters, and must have and comply with an anti-money laundering and counter-terrorism financing program. Part 11 of the Act provides that the Australian Taxation Office and certain other 'designated agencies' may access AUSTRAC information. 'Designated agencies' include a large number of Australian Government agencies as well as some state and territory agencies. The Act requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of AUSTRAC information.

10.47 The AML/CTF Act is the result of an extensive consultation process and has been the subject of a number of recent inquiries. The ALRC, therefore, restricts its consideration of the Act to issues raised in submissions to this Inquiry. The ALRC proposes that a statutory review of the AML/CTF Act should consider a number of matters, including whether reporting entities and designated agencies are appropriately handling personal information under the legislation.

10.48 The ALRC also proposes that the AML/CTF Act should be amended to provide that state and territory agencies that access personal information provided to AUSTRAC under the Act be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of the relevant obligations in the *Privacy Act.*

Interaction with state and territory laws

10.49 Chapter 14 considers how the *Privacy Act 1988* (Cth) interacts with state and territory privacy laws.

10.50 State and territory laws are sometimes inconsistent with the *Privacy Act* and with each other. Legislation regulates personal information at the federal level and in New South Wales, Victoria, Tasmania, the ACT and the Northern Territory. Queensland and South Australia have adopted administrative regimes for the management of personal information in their state public sectors. Western Australia does not have a legislative scheme to regulate personal information. State freedom of information legislation and public records legislation, however, provide some privacy protection.[3]

10.51 Further, legislation in New South Wales, Victoria and the ACT regulates health information in the public and private sectors. These Acts overlap substantially with the private sector provisions of the *Privacy Act*. Regulation of health information in other jurisdictions is restricted to public sector agencies or is the subject of codes and guidelines. Inconsistency and fragmentation in health privacy regulation is discussed in Part H.

Federal, state and territory regimes that regulate personal information

10.52 There is inconsistency in the coverage of the *Privacy Act* and the state and territory schemes. For example, state-owned corporations, ministers, universities and local governments are regulated under privacy regimes in some states and territories, but not others. The types of personal information regulated at the federal, state and territory level also differs. For example, employee records are excluded from the operation of the *Privacy Act*. Some state and territory privacy regimes, however, provide limited protection of employee records.

10.53 Although the IPPs, NPPs and privacy principles under state and territory privacy regimes are similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs.

10.54 The nature and functions of privacy regulators vary across the jurisdictions. For example, the *Privacy Act* and other federal legislation provide the Privacy Commissioner with a number of powers and functions, including powers to investigate and conciliate complaints, and approve and monitor privacy codes and guidelines.

---

3 On 28 March 2007, the Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information by the public and private sectors in Western Australia.

Although most states and territories have privacy regulators, their nature and functions vary widely. For example, the Privacy Committee of South Australia's powers and functions are limited compared to the federal, New South Wales and Victorian privacy commissioners.

10.55 The remedies available to individuals whose privacy rights are infringed can differ according to the jurisdiction in which the complaint is made. For example, the maximum amount of compensation that is payable for an interference with privacy differs across the states and territories.

10.56 As noted above, in Chapter 4 the ALRC proposes that the states and territories enact privacy laws that apply the proposed UPPs and the *Privacy (Health Information) Regulations* to regulate the public sector in that state or territory. In the ALRC's view, the adoption of the UPPs and the *Privacy (Health Information) Regulations* at the federal, state and territory level will go a long way to addressing inconsistency in the regulation of personal information.

Privacy rules, codes and guidelines

10.57 Various privacy rules, codes and guidelines regulate the handling of personal information in addition to the *Privacy Act* and state and territory legislation. Sometimes privacy rules, codes and guidelines are required by legislation. Sometimes, however, particular industries or sectors choose to develop guidelines.

10.58 A number of stakeholders noted that if rules, codes and guidelines are not aligned with the *Privacy Act*, they can contribute to inconsistency and fragmentation. On the other hand, it was also noted that additional privacy rules, codes and guidelines can clarify sector-specific issues and provide more detailed protection for personal information where appropriate.

10.59 In the ALRC's view, when agencies and organisations are developing privacy rules, codes and guidelines they should consult with the relevant body responsible for privacy for their industry or sector to ensure that the rules, codes or guidelines will interact and operate effectively with existing privacy laws.

Residential tenancy databases

10.60 Chapter 14 also discusses residential tenancy databases (RTDs). RTDs are electronic databases operated by private companies that contain information about tenants and their rental history. The purpose of such databases is to enable real estate agents to assess 'business risk' on behalf of the property owner. The listings on the database are based on information provided by real estate agents to the database operators. Listings are generally collected from across Australia and can be accessed nationally.

10.61 A number of inquiries have recognised the need for national consistency in the regulation of RTDs. As RTDs contain personal information, they are generally subject

to the private sector provisions of the *Privacy Act*. They are also regulated by legislation in some states and territories. While the states and territories can regulate the actions of the lessors and agents in their jurisdictions, they lack the power to regulate effectively the RTD operators based in other jurisdictions.

10.62 Submissions raised a number of concerns about the operation of RTDs, including that prospective tenants will often have little choice but to consent to a real estate agent passing information on to RTD operators, that information stored on RTDs is sometimes inaccurate, and that tenants sometimes have difficulties in finding out whether they are listed on RTDs. The ALRC also heard that inconsistent state and territory legislation in relation to RTDs causes a number of problems.

10.63 In the ALRC's view, the states and territories should enact legislation that addresses the relationship between the agent and the tenant, including issues such as informing the tenant of the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs.

10.64 Further, the ALRC considers that all RTD operators should be regulated by the *Privacy Act*, regardless of whether they are small business operators or whether they gain consent for the collection or disclosure of an individual's personal information. The ALRC does not propose a binding code to regulate RTD operators, however, the OPC should continue to monitor the use and operation of RTDs in order to determine whether it should exercise its proposed power to impose a binding code on RTD operators.

Part C

Interaction, Inconsistency and Fragmentation

11. The Costs of Inconsistency and Fragmentation

Contents

Introduction 419
Sharing information 420
ALRC's view 422
Compliance burden and cost 428
Do privacy laws cause an unjustified compliance burden? 430
Quantifying the compliance burden 432
ALRC's view 433
Multiple regulators 435
Submissions and consultations 435
ALRC's view 437
Government contractors 438
Commonwealth contracts 438
National consistency issues 441
State and territory contractors 443

Introduction

11.1 This chapter discusses some specific problems caused by inconsistency and fragmentation in privacy regulation in Australia. The chapter first considers how inconsistent and fragmented privacy laws can result in reluctance by organisations and agencies to share information. Secondly, the compliance burden and cost caused by inconsistent privacy requirements across jurisdictions and sectors is discussed. Thirdly, the chapter considers problems caused when particular agencies and organisations are required to comply with multiple layers of privacy regulation that is overseen by more than one regulator. Finally, the chapter outlines various issues related to government contractors.

Sharing information

11.2 In the Issues Paper *Review of Privacy* (IP 31), the ALRC asked whether the multi-layered regulation of personal information acts as a barrier to the sharing of information between agencies and organisations.[1]

11.3 Inconsistent, fragmented and multi-layered privacy regulation can contribute to confusion about how to achieve compliance with privacy regulation. This, in turn, can result in reluctance by agencies and organisations to share information.[2]

11.4 The Office of the Privacy Commissioner (OPC) submitted that some obstacles to appropriate information sharing between agencies and organisations may arise either from misapplication or a 'risk-averse' interpretation of privacy laws.[3] The ALRC heard numerous examples of agencies and organisations using 'because of the *Privacy Act*' as an excuse for not providing information.[4] In many cases, however, the *Privacy Act 1988* (Cth) would not have prohibited the sharing of the information. For example, a member of the public reported that:

> My daughter attends a childcare centre in my local area. One day, the carer commented on how well she was playing with a special friend. When I asked who the special friend was, I was advised that the name of the child, even the first name, couldn't be released to me due to the provisions of the *Privacy Act*. This is crazy.[5]

11.5 The complexity of privacy laws can act as a barrier to information sharing between federal, state and territory agencies,[6] and between agencies and organisations.[7] For example, the Office of the Victorian Privacy Commissioner (OVPC) submitted that information sharing can be problematic where federal agencies such as Centrelink, the Australian Taxation Office and the Electoral Commissioner want bulk access to state datasets because:

---

1 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–1.

2 This phenomenon is not peculiar to Australia. See, eg, M Apuzzo, 'Privacy Law Confusion Impedes Sharing', *The Daily Texan* (online), 14 June 2007, <www.dailytexanonline.com>; T Tsunetsugu and A Nakamura, 'Personal Information Law Taken Too Literally', *Daily Yomiuri*, 7 April 2007, <www.yomiuri.co.jp>; 'Stop Using the Privacy Act as an Excuse to Do Nothing', *New Zealand Herald* (online), 6 May 2007, <www.nzherald.co.nz>.

3 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

4 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also I Cuncliffe, *Submission to Senate Legal and Constitutional Affairs Committee Inquiry into the Privacy Act*, 22 February 2005.

5 National Privacy Phone-In Comment No 607, June 2006.

6 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

7 See, eg, Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007.

- some states have no privacy law and so provide the information;
- other states have privacy or other legislative provisions restricting disclosure to jurisdictions that do not have adequate privacy protection in place; and
- the Commonwealth can override privacy protection in state legislation to collect and use datasets in ways not authorised under or anticipated by state law.[8]

11.6 The Queensland Government noted that there is some evidence of inconsistency in privacy regulation affecting national schemes involving the participation of state and territory agencies.

> For example, Queensland Transport's participation in the National Exchange of Vehicle Driver Information System (NEVDIS). Queensland Transport has experienced resistance from counterpart agencies in other states with privacy legislation regarding sharing of information.[9]

11.7 A number of submissions noted that a failure to share information because of privacy concerns can impede investigations by law enforcement bodies,[10] result in decisions in family law matters being made without a complete picture of family circumstances,[11] and can have other grave consequences.[12]

11.8 The complexity of privacy laws are a particular issue in the context of service provision to vulnerable people.[13] The Community Services Ministers' Advisory Council (CSMAC) has noted that the range of differing privacy regimes across Australia creates problems for information exchange between jurisdictions, including in the critical area of child protection, where state and territory specific legislation applies. Issues also arise in relation to information exchange within jurisdictions, where some non-government welfare organisations are subject to the *Privacy Act*, and state and territory agencies must comply with state and territory regimes. CSMAC has noted that this inconsistency creates difficulties in relation to the development of

---

8 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

9 Queensland Government, *Submission PR 242,* 15 March 2007.

10 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007. See also CrimTrac, *Submission PR 158,* 31 January 2007; Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 225–226.

11 Family Law Council, *Submission PR 269,* 28 March 2007.

12 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007. A number of inquiries have considered this issue: see, eg, M Palmer, *Report of the Inquiry into the Circumstances of the Immigration Detention of Cornelia Rau* (2005) Report to the Australian Government Minister for Immigration and Multicultural Affairs. See also Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

13 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

memoranda of understanding and other protocols governing the exchange of information.[14]

11.9 Real or perceived restrictions on information sharing by agencies can also impact on business. The Taskforce on Reducing Regulatory Burdens on Business noted that barriers to sharing data between different agencies can mean that businesses are often required to supply the same information to multiple agencies, which can contribute to compliance cost.[15]

ALRC's view

11.10 The ALRC's view is that inconsistency and fragmentation in privacy laws should not prevent appropriate information sharing. Information sharing opportunities, which are in the public interest and recognise privacy as a right to be protected, should be encouraged. Rather than preventing appropriate information sharing, privacy laws and regulators should encourage agencies and organisations to design information-sharing schemes that are compliant with privacy requirements or, where necessary, seek suitable exemptions or changes to legislation to facilitate information-sharing projects.

11.11 The ALRC makes a number of proposals in relation to information sharing throughout this Discussion Paper. Perhaps the most significant of these proposals is the adoption of the proposed Unified Privacy Principles (UPPs) at the federal, state and territory level.[16] It is the ALRC's view that many of the real and perceived impediments to information sharing would be removed if the federal public sector, the state and territory public sectors and the private sector were required to comply with the same set of privacy principles. Adoption of the same privacy principles would also simplify the task of developing information-sharing protocols and memoranda of understanding. Other relevant proposals include:

- insertion of an objects clause in the *Privacy Act*, which stipulates that one of the objects of the Act is 'appropriate information sharing';[17]
- redrafting the Act to achieve greater logical consistency, simplicity and clarity;[18]
- amending the 'Use and Disclosure' principle to permit the use and disclosure of a person's information for a secondary purpose where there is a threat to a person's life, health or safety that is serious (even if not necessarily imminent);[19]

---

14 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.
15 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.
16 See Ch 4.
17 Proposal 3–4.
18 Proposal 3–2.
19 Proposal 22–3.

- the inclusion of a new exception to allow the sharing of personal information (including sensitive information) for the purposes of non-medical research;[20] and

- the adoption of the *Privacy Act* provisions that allow public interest determinations and temporary public interest determinations in state and territory laws regulating the public sectors.[21]

Education

11.12 Submissions to the Inquiry have established that many agencies and organisations are not aware of, or do not understand, their obligations under the *Privacy Act* and other such laws. This can have a 'chilling effect' on information sharing. The NSW Independent Pricing and Regulatory Tribunal (IPART) identified similar issues in its report *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency*. IPART recommended that the NSW Government provide guidance to agencies on privacy requirements affecting information sharing between agencies.[22]

11.13 The ALRC proposes that the OPC provide further guidance to agencies and organisations on privacy requirements affecting information sharing. This guidance should explain how the privacy principles operate to allow or prevent the sharing of information in certain circumstances; when a public interest determination, temporary public interest determination or a code will be appropriate; when a privacy impact assessment should be prepared; and guidance on the development of memoranda of understanding and protocols in relation to information sharing schemes. This guidance could be prepared in consultation with other bodies with responsibility for information privacy, including state and territory privacy regulators and industry-specific dispute resolution schemes.

Proposal 11–1 The Office of the Privacy Commissioner should provide further guidance to agencies and organisations on privacy requirements affecting information sharing.

Guidelines and protocols

11.14 Legislation and public interest determinations that provide for information-sharing programs will not always document how agencies should implement those

20 See Proposal 58–2.
21 See Proposal 4–4.
22 Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 228.

programs and protect personal information. Agencies that are required or authorised by legislation or a public interest determination to share personal information should, therefore, develop and publish documentation that addresses the sharing of such information. This documentation may include guidance to assist officers to implement an information-sharing scheme and protocols that detail how an agency can share information in compliance with privacy requirements.

11.15 Agencies are sometimes required to prepare other documentation in relation to information sharing. This documentation could include ministerial agreements to share information or memoranda of understanding between agencies. In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96) the ALRC considered the legislative scheme establishing the National Criminal Investigation DNA Database, a national DNA database administered by the CrimTrac agency. The ALRC recommended that for the purpose of achieving greater transparency, the Commonwealth, States and Territories should publish all ministerial agreements for sharing genetic information required under the scheme,[23] as well as protocols for inter-jurisdictional matching.[24]

11.16 In the ALRC's view, other documents (including memoranda of understanding and ministerial agreements) should also be published for the purpose of achieving greater transparency. The ALRC notes that it will not always be appropriate to publish this documentation, particularly where publication may disclose commercial-in-confidence or sensitive information.

Proposal 11–2 Agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information; and where appropriate, publish other documents (including memoranda of understanding and ministerial agreements) relating to the sharing of personal information.

---

23 Some state crimes legislation provides for the responsible minister in that state to enter into an arrangement with an Australian Government minister or with CrimTrac to provide for the transmission of information recorded in a state DNA database system to form part of the National Criminal Investigation DNA Database: see, eg, *Crimes (Forensic Procedures) Act 2000* (NSW); *Crimes Act 1958* (Vic); *Criminal Law (Forensic Procedures) Act 2007* (SA). The Minister for Justice and Customs, Senator David Johnston, has recently announced that state and territory police ministers have signed a landmark agreement on the sharing of DNA information: D Johnston (Minister for Justice and Customs), 'National DNA Sharing Arrangement Signed' (Press Release, 28 June 2007).

24 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 40–4.

Inter-agency working groups

11.17 Throughout this Inquiry, the ALRC has heard examples of agencies from various portfolios meeting to discuss information-sharing needs and how these can be accommodated under privacy legislation. In each of these cases, it appeared that a regular dialogue through an inter-agency working group facilitated information sharing while still allowing for the privacy of individuals to be accommodated.[25]

11.18 In its report, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency*, IPART considered how regulation in NSW, including privacy regulation, has the potential to impede information sharing. IPART concluded that the NSW Government should

> [c]onvene an inter-agency working group of senior officers (including representatives from Privacy NSW) to identify further opportunities where it would be appropriate (ie, where it would provide net benefits to the community) to share or streamline information among government agencies. This may require an initial stock-take or inventory of current government information requirements.[26]

11.19 As noted above, the ALRC encourages information-sharing opportunities that are in the public interest and that lessen compliance burdens on agencies, businesses and the community. In the ALRC's view, the Australian Government should take the lead in identifying circumstances where it would be appropriate to share or streamline the sharing of personal information among Australian Government agencies. The ALRC, therefore, proposes that the Australian Government should convene an inter-agency working group of senior officers, which should include a representative from the OPC to ensure the privacy interests of individuals are represented.

Proposal 11–3 The Australian Government should convene an inter-agency working group of senior officers to identify circumstances where it would be appropriate to share or streamline the sharing of personal information among Australian Government agencies.

Information sharing by law enforcement and intelligence agencies

11.20 Government agencies across the world are increasingly searching for new ways to prevent and solve crime, particularly when associated with terrorism.[27] These new

---

25 See, eg, Tasmanian Ombudsman and Health Complaints Commissioner, *Consultation*, Hobart, 40 March 2007.

26 Independent Pricing and Regulatory Tribunal of New South Wales, *Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency: Other Industries—Final Report* (2006), 228.

27 See J Lye and T McNeilly, 'Current Privacy Issues in National Security' (Paper presented at Australian Institute of Administrative Law 2006 National Administrative Law Forum, Surfers Paradise, 22–23 June 2006).

methods include new forms of intelligence gathering and the sharing of personal information, often across state and territory borders.[28]

11.21 The exchange of personal information between Australian Government agencies and state and territory government agencies for law enforcement purposes is, in most instances, regulated by privacy legislation or administrative schemes.[29] There are, however, a number of exceptions and exemptions that apply to law enforcement and intelligence agencies. For example, the Information Privacy Principles (IPPs) do not apply to the acts and practices of certain Australian Government law enforcement and intelligence agencies such as the Australian Crime Commission (ACC), the Australian Security and Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS).[30] While some of these agencies are regulated by statutory guidelines that address the handling of personal information, the guidelines do not address interjurisdictional information sharing.[31]

11.22 Further, various provisions of the *Privacy Act* exempt agencies from the operation of privacy principles in relation to their disclosure of information in response to requests received from the ACC, ASIO or ASIS and in relation to their use and disclosure of information that originated with or has been received from the ACC, ASIO or ASIS.[32]

11.23 Outside these provisions, it is necessary for agencies that are not exempt under the Act to rely on a number of broad exceptions set out in the IPPs including where use or disclosure of personal information is required or authorised by or under law, where use or disclosure is reasonably necessary for the enforcement of the criminal law, and where there is a reasonable belief that use or disclosure if necessary to prevent or lessen a serious and imminent threat to life or health.[33]

11.24 State and territory privacy regimes often provide similar exemptions and exceptions in relation to state and territory law enforcement agencies. For example, under the *Privacy and Personal Information Protection Act 1998* (NSW), a NSW government agency is not required to comply with certain privacy principles if the handling of personal information is reasonably necessary for law enforcement purposes.[34]

---

28 See, eg, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth); *Anti-Terrorism Act (No 2) 2005* (Cth); *Aviation Transport Security Act 2004* (Cth).

29 See discussion of state and territory privacy regimes in Ch 2.

30 See discussion in Ch 31.

31 These guidelines are discussed in Chs 31 and 34. These agencies are also subject to oversight by the Inspector General of Intelligence and Security or the Australian Commission for Law Enforcement Integrity.

32 See, eg, *Privacy Act 1988* (Cth) s 7.

33 The ALRC makes a number of proposals in relation to these exceptions in Part D.

34 *Privacy and Personal Information Protection Act 1998* (NSW) s 23. See also *Information Privacy Act 2000* (Vic) s 13.

11.25 In some jurisdictions, privacy regulators have developed codes and guidelines in relation to the handling of personal information by law enforcement agencies.[35] However, these documents do not deal with interjurisdictional information sharing. Further, law enforcement agencies in some jurisdictions are not subject to any privacy regulation.[36]

11.26 Should the Australian Government develop a framework for the sharing of personal information between Australian Government, and state and territory law enforcement and intelligence agencies? The United States Government recently released the *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (the Guidelines).[37] The Guidelines reflect 'basic privacy protections', requiring agencies to: identify, among other things, any privacy-protected information to be shared; assess and document applicable legal and policy rules and restrictions; put in place accountability and audit mechanisms, implement data quality and, where appropriate, redress procedures; and appoint a Privacy Official to ensure compliance with the Guidelines.[38]

11.27 The ALRC acknowledges that the broader social interest in national security and law enforcement issues will often override privacy interests. In the ALRC's view, however, in the absence of comprehensive rules to deal with the sharing of personal information between federal, state and territory law enforcement and intelligence agencies, the Australian Government should develop a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies. In the interest of transparency, this framework should be made available to the public.

11.28 This framework should be developed in consultation with relevant bodies including state and territory governments, intelligence agencies, law enforcement agencies, and various accountability bodies. These accountability bodies include the

---

35 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001); Office of the NSW Privacy Commissioner, *Privacy Code of Practice: Law Enforcement and Investigative Agency Access to Personal Information Contained in Public Registers*.

36 See discussion in Ch 2 and Ch 14.

37 United States Government Office of the Director of National Intelligence, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (2006). The 'Information Sharing Environment' has been described as 'the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of all federal executive branch entities to facilitate terrorism information sharing, access, and collaboration among users in order to combat terrorism more effectively': Program Manager—Information Sharing Environment, *Information Sharing Environment Privacy Guidelines—Frequently Asked Questions* (2006) Unites States Government Office of the Director of National Intelligence <www.ise.gov> at 31 July 2007.

38 Program Manager—Information Sharing Environment, *Information Sharing Environment Privacy Guidelines—Frequently Asked Questions* (2006) Unites States Government Office of the Director of National Intelligence <www.ise.gov> at 31 July 2007.

OPC, state and territory privacy commissioners and agencies with responsibility for privacy regulation; as well as bodies with responsibility for overseeing law enforcement and intelligence agencies, including the Australian Commission for Law Enforcement Integrity and the Inspector-General of Intelligence and Security, and federal, state and territory ombudsmen. The ALRC also proposes the development of memoranda of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

Proposal 11–4 The Australian Government, in consultation with: state and territory governments, intelligence agencies, law enforcement agencies, and accountability bodies (including the Office of the Privacy Commissioner; the Inspector-General of Intelligence and Security; the Australian Commission for Law Enforcement Integrity; state and territory privacy commissioners and agencies with responsibility for privacy regulation; and federal, state and territory ombudsmen), should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memoranda of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

Compliance burden and cost

11.29 The Terms of Reference for this Inquiry require the ALRC to consider 'the desirability of minimising the regulatory burden on business'. Business has identified the pervasive nature of privacy requirements as an important contributor to the cumulative regulatory burden it faces.[39] The Australian Chamber of Commerce and Industry has reported that, in response to its 2004 Pre-Election Survey, 47.4% of Australian businesses polled considered that compliance with privacy requirements was a problem.[40]

11.30 The Taskforce on Reducing Regulatory Burdens on Business (the Regulatory Taskforce) heard that inconsistency in the areas of workplace surveillance, direct marketing and telemarketing laws, and having to supply information to multiple

39 See, eg, Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 54.

40 Australian Chamber of Commerce and Industry, *Submission to the Taskforce on Reducing Regulatory Burdens on Business*, 1 November 2005, 5.

government agencies, contributed to compliance burdens and costs.[41] The OPC review of the private sector provisions of the *Privacy Act* (OPC Review) was told that the lack of a single, national and comprehensive regime makes compliance more difficult and that the complexity of federal privacy laws (including the *Privacy Act* and the *Telecommunications Act 1997* (Cth)) contributes to compliance costs.[42]

11.31 The Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (the Senate Committee privacy inquiry), however, heard conflicting views in relation to compliance burden and cost.[43] A number of submissions to the Committee's inquiry noted the considerable compliance costs associated with privacy regulation, including for small not for profit organisations.[44] It was argued in other submissions, however, that the benefits of privacy regulation to business and Australian society outweigh the costs of compliance.[45] The Australian Consumers Association submitted that it had little sympathy with complaints about compliance costs arising from privacy legislation, noting that there is no required reporting or mandatory recording under the schemes.[46]

11.32 The Regulatory Taskforce noted that achieving nationally consistent privacy laws is an important factor in reducing compliance costs for business.[47] The Regulatory Taskforce recommended that the Australian Government ask the Standing Committee of Attorneys-General (SCAG) to endorse national consistency in all privacy-related legislation based on the concept of minimum effective regulation.[48] In its response, the Australian Government stated that:

---

41 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 53–57.

42 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 36–37, 66.

43 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.149]–[4.154].

44 Ibid, [4.152].

45 Ibid, [4.150]. See also H Pearson, 'Privacy Is Good For Business', *CEO Forum*, 18 April 2007, <www.ceoforum.com.au>.

46 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.149]–[4.154].

47 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), [4.151].

48 Ibid, rec 4.47.

> The Australian Government agrees to the recommendation and supports the goal of national consistency in privacy-related legislation. At the April 2006 meeting of the Standing Committee of Attorneys-General, Attorneys-General agreed to establish a working group to advise Ministers on options for improving consistency in privacy regulation, including workplace privacy.[49]

11.33 The recent Productivity Commission report, *Performance Benchmarking of Australian Business Regulation*, found that there is evidence that significant differences in compliance cost levels exist across jurisdictions. The Productivity Commission concluded that the benchmarking of regulatory burdens across jurisdictions could shed light on where and how such differences might be reduced and increase government accountability for the design, administration and enforcement of regulation.[50]

Do privacy laws cause an unjustified compliance burden?

11.34 In IP 31, the ALRC asked whether the multi-layered regulation of personal information causes an unjustified compliance burden.[51] The ALRC received a large number of submissions that claimed that the proliferation and fragmentation of privacy laws have increased compliance burden and cost for both agencies and organisations.[52] A number of submissions identified that state health privacy legislation and workplace surveillance laws are creating complexity and unjustified compliance costs.[53] It was also noted that compliance burden is a particular issue for small businesses that are required to comply with the *Privacy Act*.[54]

---

49 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

50 Australian Government Productivity Commission, *Performance Benchmarking of Australian Business Regulation* (2006), 156. The Productivity Commission has since announced that it will undertake a series of annual reviews of regulatory burdens on business under Australian Government regulation. It is not clear when privacy regulation will be reviewed: Productivity Commission, *Annual Review of Regulatory Burdens on Business—Primary Sector*, Productivity Commission Circular, 28 February 2007.

51 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–1.

52 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Health Insurance Association, *Submission PR 161,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007; D Antulov, *Submission PR 14,* 28 May 2006.

53 See, eg, Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Cancer Council Victoria, *Consultation PC 75*, Melbourne, 5 February 2007. A Standing Committee of Attorneys-General working party is currently considering workplace privacy: see Chs 1 and 2.

54 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007. See also Ch 35.

11.35 The OVPC submitted that there is little evidence of the existence or extent of any compliance burden. It noted, however, that compliance burden is most likely to be a problem for organisations that do not have the resources to get advice and training about their privacy obligations, especially where they are working in an area that intersects with multiple privacy regimes. This often has an impact on service providers, especially where they receive joint Commonwealth-state funding.[55]

11.36 The OPC submitted that, in many areas, the compliance obligations are proportionate and appropriate to public expectations. It noted, for example, that the *Privacy Act* requires agencies and organisations to take actions that are 'reasonable' to fulfil obligations relating to notice requirements, data quality and data security. What is considered 'reasonable' is contextual, and may depend on the entity's size and activities. The OPC stated, however, that it recognised that compliance costs escalate where entities must comply with multiple layers of privacy regulation, and suggested that

> the solution may be to resolve questions of jurisdiction. For example, by clarifying that the Privacy Act 'covers the field' of the private sector to the exclusion of other jurisdictions' privacy legislation. In other cases, governments and regulators may work together to promote greater consistency between regulations and administrative procedures, without disrupting existing regulatory frameworks.[56]

11.37 Inconsistency and fragmentation in privacy regulation are a problem for organisations that operate in more than one Australian jurisdiction. For example, the OPC Review was told by one organisation that operates nationally that

> a single piece of personal information may be subject to two or more … legislative regimes at one time, creating conflicting obligations, different obligations or more onerous obligations in respect of the whole or parts of that same piece of information.[57]

11.38 The OPC Review also cited an instance where a national medication service operating via a call centre had to read different statements to obtain consent depending on the location of the individual (and the law that applied in that state or territory).[58] The Regulatory Taskforce also noted that this was an issue in the context of different laws relating to direct marketing.[59]

---

55 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
56 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
57 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 40.
58 Ibid, 66.
59 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 54.

11.39 Submissions to this Inquiry noted that the main issues for national organisations are compliance burden and cost.[60] In particular, differences in rules governing acceptable calling times for telemarketers, and state and territory laws dealing with the privacy of employee records, were highlighted as particularly problematic.[61] Other submissions noted that state health privacy legislation is creating problems for national organisations.[62] The OPC submitted that in some cases these problems are

> an inevitable consequence of large-scale operations across a federal system, which national organisations are often better equipped to deal with due to their size. In particular sectors, including health, greater consistency in regulation would clarify obligations and may facilitate the implementation of interstate and national initiatives.[63]

11.40 Multi-layered regulation of personal information complicates the implementation of programs and services at a national level.[64] Submissions noted that this is particularly an issue in the health sector,[65] where it is creating a compliance burden and impacting on quality in the health care and health and medical research sectors.[66] The Australian Bureau of Statistics stated that complex and overlapping legal requirements across jurisdictions make it difficult to collect and use state and territory administrative data for statistical purposes.[67] The Australian Government Department of Human Services submitted that:

> Projects such as the Access Card need to navigate their way through complex and competing legislation covering federal and state public sector and in some instances the private sector. This in turn slows implementation and significant community benefits.[68]

Quantifying the compliance burden

11.41 In IP 31, the ALRC noted that it would be interested in receiving information that can quantify the compliance burden experienced due to problems associated with privacy regulation.[69] Stakeholders submitted that inconsistent privacy laws create a compliance burden in the following areas: monitoring changes to the law, staff training, changing internal policies and procedures, rewriting privacy policies and

---

60 See, eg, AAMI, *Submission PR 147,* 29 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007; D Antulov, *Submission PR 14,* 28 May 2006.

61 Telstra, *Submission PR 185,* 9 February 2007; AAMI, *Submission PR 147,* 29 January 2007.

62 AAMI, *Submission PR 147,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

63 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

64 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–1(c).

65 See, eg, Australian Commission on Safety and Quality in Health Care, *Consultation*, Sydney, 27 November 2006.

66 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

67 Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

68 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

69 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [7.11].

consumer information, and lost business due to a consumer perception of a lack of service.[70] One submission noted that many of these costs are ongoing due to continuous changes in federal, state and territory legislation.[71]

11.42 Based on a survey it conducted for the OPC Review, the Australian Chamber of Commerce and Industry estimated that the legal costs for drafting a rudimentary privacy policy in 2007, tempered by the fact that the cost could vary considerably depending upon the characteristics of the business, were approximately $2500.

> Supporting documentation, in terms of reference material such as the Federal Privacy Handbook and the Privacy Toolkit would now cost an additional $1000. This represents a base cost of $3,500 for an individual business. Using the latest available data, when multiplied across the 1.8 million businesses with a turnover of less than $2 million, or by the 1.9 million businesses classified as small businesses, this results in an aggregate cost to the economy of $6.3 billion or $6.65 billion dollars, or roughly 0.7 per cent of gross domestic product.
>
> Ongoing costs would include implementation of the policy, staff training, updating of the policy and dealing with inevitable complaints (legitimate or otherwise), all of which would entail significant costs in terms of staff time and business resources.[72]

11.43 Submissions noted that compliance costs are often passed on to the consumer.[73] These costs are not always financial. For example, the National Health and Medical Research Council (NHMRC) submitted that the multi-layered level of privacy laws will sometimes prevent information exchange for the purpose of medical research. This can compromise clinical care, quality assurance and related activities because access to essential health information is impaired; significant research is not approved or submitted for approval; additional requirements are imposed on some research that reduce its scientific rigour; and excessive administrative effort and costs are incurred.[74]

ALRC's view

11.44 The ALRC's view is that some of the compliance burden imposed by the *Privacy Act* is justified. The *Privacy Act* was enacted to implement Australia's obligations relating to privacy under the *International Convention on Civil and Political Rights* as well as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of*

---

70 See, eg, Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; AAMI, *Submission PR 147,* 29 January 2007; Australasian Compliance Institute, *Submission PR 102,* 15 January 2007.

71 Australasian Compliance Institute, *Submission PR 102,* 15 January 2007.

72 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

73 Australasian Compliance Institute, *Submission PR 102,* 15 January 2007.

74 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007. See also CSIRO, *Submission PR 176,* 6 February 2007.

Personal Data.[75] It was, therefore, enacted to protect a fundamental human right—the right of an individual to privacy.

11.45 The compliance requirements under the Act are minimal when compared to comparable schemes in Europe that often include an expensive registration requirement. The *Privacy Act* does not have extensive reporting requirements such as under the *Corporations Act 2001* (Cth). Further, as noted by the OPC, the Act can take account of an agency or organisation's size and activities. The ALRC also notes that the OPC is available to provide guidance to agencies and organisations free of charge.

11.46 In Chapter 35, the ALRC proposes the removal of the small business exemption under the *Privacy Act*. Stakeholders have expressed concern about the compliance burden on small businesses. The ALRC therefore proposes that, before the removal of the exemption, the OPC should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by establishing a national small business hotline; developing plain English educational materials; and developing and publishing templates for small businesses to assist in preparing Privacy Policies.

11.47 In the ALRC's view, however, inconsistency and fragmentation in the regulation of personal information at the federal, state and territory level does create an unjustified compliance burden. Time and money can be spent identifying sources of privacy obligations and complying with disparate law and inconsistent privacy standards in different jurisdictions. This problem is acute when implementing programs and services by agencies and organisations at a national level. The costs associated with this burden are both financial and social.

11.48 The ALRC makes a number of proposals throughout this Discussion Paper that are intended to minimise inconsistency and fragmentation, and streamline the regulation of personal information. For example, as outlined above, the ALRC proposes the amendment of the *Privacy Act* to clarify the scope of the Act in relation to the private sector; the adoption of a single set of privacy principles at the federal, state and territory level; and a redraft of the *Privacy Act* to minimise its complexity. The ALRC also makes a number of proposals to clarify the interaction of different laws that regulate the handling of personal information, particularly laws that regulate the health sector, credit reporting, and the telecommunications industry.[76]

11.49 The ALRC also proposes a greater emphasis on the OPC's educative role including by issuing guidance about the interaction of the *Privacy Act* with other federal, and state and territory laws that regulate the handling of personal information. Parts F and J also include a number of proposals directed to encouraging greater

---

75 See discussion in Ch 4.

76 See Part G (Credit Reporting Provisions), Part H (Health Services and Research) and Part J (Telecommunications).

cooperation between privacy regulators and other bodies with responsibility for privacy.

Multiple regulators

11.50 Some industries are required to comply with multiple layers of privacy regulation overseen by more than one regulator. This has been identified as an issue in the telecommunications industry[77] and the financial services sector. For example, bank customers with privacy complaints may choose to lodge a complaint with the Banking and Financial Services Ombudsman (BFSO) or the OPC. A financial services organisation has reported that multiple regulators can work well together when there is effective communication and coordination.[78]

11.51 In IP 31, the ALRC noted that industry ombudsmen and the OPC may take opposing views in relation to the same privacy complaint. Concerns were expressed to the OPC Review about the lack of clarity in the respective complaint handling responsibilities of the federal and NSW privacy commissioners,[79] and that consumers may not know which regulator to complain to or which law applies to their matter.[80]

Submissions and consultations

11.52 In IP 31, the ALRC asked whether the multi-layered regulation of personal information handling raises any issues in relation to the existence of multiple privacy regulators in particular industry sectors and across the states and territories.[81]

11.53 Stakeholders noted that the lack of consistency of federal and state and territory privacy regimes leads to confusion about where and how to complain,[82] and that it would be useful to have a 'one-stop shop' for complaint handling.[83]

11.54 A number of organisations reported that the existence of multiple regulators also increases the compliance cost to business by increasing the number of 'compliance

---

77 See discussion in Ch 10 and Telstra, *Submission PR 185,* 9 February 2007; Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, 9.

78 ANZ, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 February 2005, 5–6.

79 Private Health Insurance Ombudsman, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 14 December 2004, 1.

80 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 68.

81 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–1(d).

82 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006.

83 Telstra, *Submission PR 185,* 9 February 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Health Consumer Council WA, *Consultation*, 25 January 2007; WA Information Commissioner, *Consultation*, 23 January 2007.

activities' required each year, duplicating effort, incurring additional expense in responding to privacy inquiries and in establishing procedures to respond to complaints, and slower resolution of issues.[84]

11.55 Privacy regulators also noted difficulties. The OVPC submitted that there will be cases where privacy regulators cannot agree on which privacy law applies.[85] The OPC noted that the existence of multiple regulatory bodies does not necessarily lead to negative outcomes. The OPC emphasised that lack of consistency in legislation is often the primary source of the problem, rather than the existence of more than one regulator.[86] The OPC observed, however, that the existence of multiple regulators at the federal, state and territory level raises three concerns.

> First, it can be difficult for individuals to understand their rights, and know how to enforce them. Second, organisations may bear increased compliance costs by having to obey multiple sets of regulations. Third, this may lead to unnecessary duplication of effort and resource expenditure by regulators.[87]

11.56 The OPC considered that the existence of multiple regulators in one sector presents the potential risks of forum shopping, inefficient use of resources, and inconsistent outcomes. The OPC was of the view, however, that these issues could be overcome by

> creating memoranda of understanding, harmonisation of complaint-handling procedures and legislative interpretation, and appropriate referral mechanisms. Where the source of these problems is inconsistent legislation, clarifying the scope of each regulator's jurisdiction could help to avoid such risks, provided this does not lead to gaps in regulatory coverage.[88]

11.57 The Australian Privacy Foundation submitted that having more than one regulator is important for 'peer review', which can contribute to the maintenance of high standards and a consumer focus. It noted, however, that it is essential that multiple privacy regulators establish a good working relationship.[89]

11.58 The need for regulators with expertise in certain industry sectors was noted in other submissions. For example, the NHMRC submitted that health privacy issues require the attention of regulators who are expert in privacy and also have specific expertise in the health services and health and medical research sectors.[90] The Australian Bankers' Association noted that the majority of the few privacy-related

---

84 Telstra, *Submission PR 185,* 9 February 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007. See also Australian Chamber of Commerce and Industry, *Holding Back the Red Tape Avalanche: A Regulatory Reform Agenda for Australia* (2005).

85 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

86 The OPC noted the inconsistency between the *Privacy Act* and NSW health privacy legislation: see Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007 and Part H.

87 Ibid.

88 Ibid.

89 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

90 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

complaints the BFSO receives are part of wider banking complaints. It is therefore convenient for the customer to have the dispute dealt with by the one body, particularly as the OPC would not have the power to determine the banking aspects of the dispute.[91]

ALRC's view

11.59 In the ALRC's view, there are a number of benefits in having multiple regulators that are responsible for privacy. It is preferable to have privacy regulators at the federal, state and territory level as it ensures that citizens in each jurisdiction have a regulator they can approach for advice and to make a complaint. Similarly, organisations that are subject to local privacy laws have access to a local regulator who is aware of their circumstances and can provide advice and training on implementing the legislation.[92]

11.60 Further, industry-specific regulators, such as the BFSO and the Telecommunications Industry Ombudsman, play an important role in the regulation of personal information handling as they provide industry expertise that the OPC does not possess. Industry-specific regulators also reduce the volume of privacy complaints that would otherwise be made to OPC, freeing the OPC's resources for other functions.

11.61 Another potential benefit is peer review and the promotion of high standards of performance. This will be facilitated by privacy regulators interpreting a single set of privacy principles, and transparency can be promoted by publishing their decisions and guidance on the operation of the principles.

11.62 The ALRC also accepts, however, that there is evidence to suggest that multiple privacy regulators can create confusion for individuals in making complaints, and for organisations and agencies in seeking advice. Further, it can create a compliance burden for businesses and result in the inefficient use of privacy regulators' resources.

11.63 The ALRC therefore makes a number of proposals that are aimed at improving the operation of multiple privacy regulators. These proposals are summarised in Chapter 10 and are aimed at achieving greater cooperation between privacy regulators.

11.64 Other relevant proposals include amending the *Privacy Act* to empower the Privacy Commissioner to delegate all or any of the powers in relation to complaint handling conferred on the Commissioner by the Act;[93] the development of memoranda of understanding between the OPC and other bodies with responsibility for privacy; and the development and publication of complaint-handling policies, enforcement

---

91 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
92 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
93 See Ch 45.

guidelines and educational material that addresses the role and functions of the various bodies with responsibility for information privacy.[94]

Government contractors

11.65 While information about federal, state and territory privacy regimes is publicly available, Australian Government, and state and territory agency contracts are not. This makes it difficult to detect whether contractual privacy provisions are inconsistent with the *Privacy Act*.[95] In IP 31, the ALRC asked whether privacy provisions in Australian Government, state or territory agency contracts contribute to inconsistency and fragmentation in privacy regulation.[96]

11.66 The OPC submitted that, in many cases, contractual privacy provisions are an appropriate way to incorporate higher privacy obligations than may otherwise apply, or to maintain privacy protections that already apply to personal information. For example, they may compel a contractor to undertake specific privacy-related activities, such as mandatory reporting of suspected privacy breaches, or to undertake staff training.[97]

11.67 The Department of Health and Ageing submitted that the standard provisions developed for inclusion in each of the Department's contracts require contractors and consultants to comply with relevant IPPs and National Privacy Principles (NPPs) or an approved privacy code in relation to their activities under the contract and to impose equivalent obligations on any subcontractor.[98]

11.68 The Australian Privacy Foundation submitted, however, that privacy clauses in contracts are often overly legalistic, claiming to cover all possibilities but too often failing to allocate clearly responsibility for breaches.[99] The National Association for Information Destruction submitted that Australian agencies have taken an inconsistent approach to documents containing information regulated by the Act.[100]

Commonwealth contracts

11.69 The *Privacy Act* imposes obligations on agencies entering into contracts to provide services to or on behalf of the agency. Section 95B requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract or a subcontractor does not do an act or engage in a

---

94 See Ch 64.

95 The Australian Government Solicitor has drafted a model clause to assist agencies in discharging their responsibilities under the *Privacy Act 1988* (Cth): Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 7–8.

96 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–2(a).

97 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

98 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

99 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

100 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

practice that would breach the IPPs. The *Privacy Act* defines a 'contracted service provider' as 'an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract', or a subcontractor for the government contract.[101]

11.70 A small business that is also a contracted service provider will be subject to the *Privacy Act* in respect of the performance of that contract.[102] A state or territory authority contracting with an agency will not be covered by the Act. A 'State contract' is defined as a 'contract, to which a state or territory or state or territory authority is or was a party, under which services are to be, or were to be, provided to a state or territory authority'.[103] Section 16F of the *Privacy Act* provides that an organisation must not use or disclose personal information for direct marketing unless the use or disclosure is necessary to meet an obligation under the contract.

11.71 An act done or practice engaged in by a contracted service provider for the purposes of meeting an obligation under a contract will not breach an NPP or an approved privacy code if the act or practice is authorised by the contract. Therefore, the NPPs or a code can be varied by the contract and a breach of an NPP or code will not have occurred if the contractual obligations require the contracted service provider to do an act or practice that would be inconsistent with an NPP or an approved code to which it is bound.[104]

11.72 The Privacy Commissioner has jurisdiction to investigate directly the action of a contractor or subcontractor. Section 13A(1)(c) provides that a breach of a 'non-complying' privacy provision in a Commonwealth contract is an interference with privacy. The standards the Privacy Commissioner would apply in investigating a complaint are those set out in the contract.[105]

11.73 The obligations under s 95B extend to a contracted service provider who is not within Australia.[106] Although the Privacy Commissioner could take action overseas to

---

101 *Privacy Act 1988* (Cth) s 6(1).

102 Ibid s 6D(4)(e).

103 The Australian Government Solicitor has advised, however, that notwithstanding this exclusion, agencies need to be mindful of the obligation under IPP 4(b) to ensure that everything reasonable is done to prevent unauthorised use or disclosure of personal information when contracting with a state or territory authority: Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

104 *Privacy Act 1988* (Cth) ss 6A(2), 6B(2). Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 5.

105 Office of the Federal Privacy Commissioner, *Privacy Obligations for Commonwealth Contracts*, Information Sheet 14 (2001).

106 *Privacy Act 1988* (Cth) s 5B.

investigate complaints, enforcement of the provisions of the contract overseas may be difficult.[107]

Submissions and consultations

11.74 In IP 31, the ALRC asked whether the *Privacy Act* provisions relating to Commonwealth contractors are appropriate and effective.[108]

11.75 The OPC noted that the *Privacy Act* does not restrict Australian Government agencies from including contractual clauses that refine existing privacy obligations, or impose additional obligations on a contractor, which may be appropriate under certain circumstances. It submitted that, in this regard, the current provisions are appropriate and effective.[109] The OPC stated, however, that the definition of 'contracted service provider' in the Act could be reviewed to ensure that it is adequate to cover all the types of activities that private sector organisations might perform on behalf of agencies.[110]

11.76 A number of stakeholders considered that the provisions are unclear and require redrafting.[111] For example, the OVPC submitted that it is not clear whether contracted service providers are able to contract out of their obligations under the NPPs or a code. The OVPC suggested that the position under the *Information Privacy Act 2000* (Vic) may be clearer in this regard—organisations cannot contract out of their privacy obligations.[112] The OVPC also noted that difficulties have arisen in relation to the enforceability of provisions that purport to contractually bind a service provider to obligations under the *Information Privacy Act*.[113]

11.77 Electronic Frontiers Australia submitted that the *Privacy Act* should be amended to place obligations on organisations that engage contractors to ensure the contractor only uses or discloses personal information given to it for the purposes for which it is given and to keep it secure. Electronic Frontiers Australia also submitted that it would not support an exemption for Commonwealth contractors that are small businesses or small business operators.[114]

---

107 Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

108 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–2(b).

109 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

110 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

111 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

112 *Information Privacy Act 2000* (Vic) s 16.

113 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

114 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

ALRC's view

11.78 In the ALRC's view, the *Privacy Act* provisions relating to Commonwealth contractors remain appropriate and effective. The ALRC notes the comments of stakeholders that the contracted service providers provisions are unclear. While the ALRC does not share this view, the redraft of the *Privacy Act* proposed in Chapter 3 may deal with these concerns.

11.79 Problems caused by government contractors being subject to two sets of privacy principles will be addressed by the proposed UPPs replacing the IPPs and NPPs. The operation of an exception to the UPPs or an exemption may, however, still result in an agency and organisation being subject to different privacy standards. The government contractor provisions of the *Privacy Act* should therefore be retained to ensure that organisations that contract with an Australian Government agency are subject to the same privacy principles as the agency itself.

11.80 Other *Privacy Act* provisions relating to government contractors should also be retained, including those relating to direct marketing and the disclosure of certain provisions of Commonwealth contracts. If the ALRC's proposal to remove the small business exemption is not implemented, a small business that is also a contracted service provider should continue to be subject to the *Privacy Act* in respect of the performance of that contract.[115]

11.81 The OPC has commented that the definition of 'contracted service provider' in the Act could be reviewed to ensure that it is adequate to cover all the types of activities that private sector organisations might perform on behalf of agencies. The ALRC did not receive any other submissions on this issue. The ALRC remains interested in views on what types of activities are not covered by the definition of 'contracted service provider', and whether the definition should be amended. The ALRC is also interested in whether the definition of 'State contract' under the Act is adequate.

Question 11–1 Are the definitions of 'contracted service provider' and 'State contract' under the *Privacy Act* adequate? For example, do they cover all the types of activities that organisations might perform on behalf of agencies?

National consistency issues

11.82 The OPC Review was told that contracted service providers can be required to comply with three sets of privacy principles—the NPPs which apply to them in their

115 See Ch 35.

capacity as private sector organisations, the IPPs which apply to them under contracts granted in accordance with s 95B of the *Privacy Act*, and any applicable state or territory privacy laws.[116] This may be an issue particularly for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies.

11.83 Telstra advised the OPC Review that the proliferation of state legislation and inconsistency between state and federal legislation can add costs to conducting business with government agencies.[117] The OPC recommended that the Australian Government consider reviewing the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations. In its view, this would address the issues surrounding government contractors.[118]

11.84 Non-government agencies receiving program funding from the Australian Government and state or territory governments may be required to comply with state privacy regimes as well as the *Privacy Act*. The OPC has reported that a charity that administers an employment services and community services program may have to comply with the NPPs and the IPPs, department procedural requirements and state or territory law. The issue is further complicated by the fact that the organisation may need to collect health information, which is subject to state or territory health records legislation.[119]

11.85 In IP 31, the ALRC asked whether any issues arise for Commonwealth contractors that are subject to the NPPs and the IPPs. The ALRC also asked whether any issues arise for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies.[120]

11.86 National consistency issues were raised in a number of submissions.[121] For example, the Government of South Australia submitted that:

> a State/Territory privacy authority may approve a Memorandum of Understanding concerning information disclosure between government-based welfare agencies to apply to service delivery in a particular circumstance, or grant an exemption to the privacy principles for a specified research study, but this cannot be extended to NGOs

116 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, 13.
117 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 37.
118 Ibid, 8 and rec 5. See Ch 15.
119 Ibid, 38.
120 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–2(c) and (d).
121 Law Council of Australia, *Submission PR 177,* 8 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

> bound by an alternative regime, though they may be partners in service delivery or hold a considerable volume of the relevant client information.[122]

11.87 A large number of stakeholders agreed that the development of a single set of principles that applied at the federal, state and territory level would deal with these issues.[123] For example, Telstra noted that contractors to state governments are not bound by privacy rules in some states, and submitted that such issues could be resolved through the introduction of a single set of privacy principles across all Australian jurisdictions.[124]

State and territory contractors

11.88 The privacy regimes in some states and territories include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs. Although the privacy principles in the various state and territory regimes often resemble the IPPs and NPPs, they are not identical.

11.89 Some state and territory privacy regimes require organisations that provide contracted services to a state or territory government agency to be bound by the relevant state privacy principles for the purposes of the contract.[125] Other state regimes provide that compliance with the state privacy regime is subject to any outsourcing arrangements,[126] or are silent on this issue.[127]

Submissions and consultations

11.90 In IP 31, the ALRC asked whether there are concerns that organisations acting under a state or territory contract may not be required to adhere to the same privacy standards that are applicable to organisations under the *Privacy Act*.[128]

11.91 The OPC submitted that it has ongoing concerns that state or territory government contractors, who are otherwise organisations, may not be bound by the *Privacy Act* or equivalent standards when performing functions under state or territory contracts. The OPC noted that the absence of consistent regulation for state contractors and the possible imposition of different obligations can create gaps in privacy

---

122 Government of South Australia, *Submission PR 187,* 12 February 2007.

123 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

124 Telstra, *Submission PR 185,* 9 February 2007. See also Law Council of Australia, *Submission PR 177,* 8 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

125 See, eg, *Information Privacy Act 2000* (Vic) s 17; *Information Act 2002* (NT) s 149.

126 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

127 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW); South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

128 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–2(e).

protections and confusion about which body should regulate the privacy practices of state contractors.

> For example, in one instance, the Office had to decline to investigate a worker's compensation matter because it involved a state contractor, but no state privacy regime existed to deal with the matter. In other cases, both the Office and state privacy bodies have declined to investigate the practices of a state contractor.[129]

11.92 The OPC submitted that state and territory contractors should be covered by the *Privacy Act*, or at least equivalent legislation. The OPC noted that this could be achieved by all states and territories enacting privacy legislation which imposes protections on their agencies and contractors that are at least equivalent to the *Privacy Act*. The OPC submitted in the alternative that s 7B(5) of the *Privacy Act* could be amended to ensure that the NPPs apply to state contractors where no equivalent state or territory privacy laws exist.[130]

11.93 The OVPC submitted that the *Privacy Act* should be amended to recognise state privacy laws may apply to contracted service providers seeking to be covered by a voluntary federal code, and to import a requirement to consult with and seek the approval of the states before any code covering state contracts is approved.[131]

ALRC's view

11.94 The Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that it was the intention of the Australian Parliament that the acts and practices of state and territory contractors would 'not be covered by the Commonwealth's privacy scheme but rather the State or Territory's own privacy standards'.[132]

11.95 In the ALRC's view, organisations that contract with a state government should be regulated by privacy legislation. In its 1998 report, *Contracting Out of Government Services*, the Administrative Review Council concluded that

> the contracting out of government services should not result in a loss or diminution of government accountability or the ability of members of the public to seek redress where they have been affected by the actions of a contractor delivering a government service.[133]

11.96 The ALRC considered proposing that the *Privacy Act* should be amended to include a 'roll-back provision' to cover state contractors. The ALRC believes, however, that such a law would intrude too heavily on state and territory government

---

129 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
130 Ibid.
131 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
132 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 8.
133 Administrative Review Council, *The Contracting Out of Government Services*, Report No 42 (1998), Executive Summary.

business. Instead, the ALRC proposes that state and territory privacy legislation should include provisions relating to state and territory contractors.[134]

11.97 In the ALRC's view, organisations would rarely seek to be covered by a code under the *Privacy Act* in relation to state contracts. The ALRC does not agree that the *Privacy Act* should be amended to include a requirement for the OPC to consult with and seek the approval of the states before any code is approved covering state contracts. This requirement will not be necessary if each state and territory introduces provisions to regulate government contractors in that jurisdiction. This issue could be addressed, however, in a memorandum of understanding between the OPC and state and territory privacy regulators.

134 See Proposal 4–4.

12. Federal Information Laws

Contents

Introduction 447
Terms and definitions 447
Freedom of Information Act 1982 (Cth) 449
Disclosure of personal information 449
Required or authorised by or under law 453
Access and correction 455
An exemption for complaint-handling files 467
Archives Act 1983 (Cth) 468
The 'personal affairs' exemption 468
The open access period 471
A single information Act? 472
A single regulator? 474
Secrecy provisions 476
Obligations of confidence 482
Common law and equitable duties of confidence 482
Statutory protection of confidential information 483
Part VIII of the *Privacy Act* 483

Introduction

12.1 This chapter considers how the *Privacy Act 1988* (Cth) interacts with a number of federal laws that regulate the handling of personal information. The chapter first considers the use of inconsistent terms and definitions across federal information laws. The chapter next discusses the interaction between the *Privacy Act*, *Freedom of Information Act 1982* (Cth) (FOI Act) and the *Archives Act 1983* (Cth), and considers whether the three Acts should be combined in the one Act and administered by a single body. The chapter then examines how the *Privacy Act* interacts with secrecy provisions in federal legislation. The final section of the chapter considers whether the confidentiality provisions in Part VIII of the *Privacy Act* are still required.

Terms and definitions

12.2 Chapter 3 considers various definitions used in the *Privacy Act* including 'personal information', 'sensitive information', 'record' and 'generally available publication'. This section of the chapter is concerned with the consistent use of terms and definitions across federal information laws.

12.3 Federal legislation other than the *Privacy Act* regulates the handling of personal information. Sometimes this legislation adopts different terms or definitions to those used in the *Privacy Act*. For example, the concept of 'personal information' is central to the regime established by the *Privacy Act*, but other federal legislation adopts different terms such as 'personal affairs' to describe similar information.[1]

12.4 The definitions of other terms used in the *Privacy Act* sometimes differ from the same terms used in other federal legislation. For example, the definition of 'consent' under the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) differs from the *Privacy Act* definition.

12.5 Terms and definitions also vary across federal, state and territory laws. For example, each of the state and territory regimes contain definitions of 'personal information' that are similar to the definition of the term under the *Privacy Act*, but not identical.[2]

12.6 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the inconsistent use of terms and definitions that regulate the handling of personal information create any difficulties.[3] Most submissions stated that federal, state and territory privacy legislation should use terms consistently.[4] A number of submissions noted that inconsistent definitions can add to the complexity of privacy laws and can lead to unjustified compliance burden and cost.[5]

12.7 The Office of the Privacy Commissioner (OPC) noted, however, that it is not aware of major difficulties in privacy regulation caused by multiple definitions for the same term and would be wary of unintended consequences arising from attempts to unify definitions inappropriately.[6]

12.8 In the ALRC's view, the inconsistent use of terms and definitions in privacy legislation contributes to the complexity of privacy law and may increase compliance burden and cost. The ALRC therefore proposes that the Australian Government should ensure the consistency of definitions and key terms (for example, 'personal

---

1 See, eg, *Archives Act 1983* (Cth) s 33.

2 See, eg, *Privacy Act 1988* (Cth) s 16B; *Privacy and Personal Information Protection Act 1998* (NSW) s 4; *Information Privacy Act 2000* (Vic) s 3; *Personal Information Protection Act 2004* (Tas) s 3; see definition of 'record' in Queensland Government, *Information Standard 42—Information Privacy* (2001); *Personal Information Protection Act 2004* (Tas) s 4. The *Freedom of Information Act 1992* (WA) refers to personal information contained in documents: see, eg, *Freedom of Information Act 1992* (WA) s 29. The South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992) refers to personal information concerning the 'record subject'. It is, however, unclear whether the instruction covers only documents in a recorded form.

3 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–4.

4 Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

5 AAMI, *Submission PR 147,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.

6 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

information', 'sensitive information' and 'health information') in federal legislation that regulates the handling of personal information.

12.9 There will be occasions, however, when other policy considerations will justify the use of terms or definitions that differ from those used in the *Privacy Act*. This is the case in relation to the use of different definitions of 'consent' under the *Privacy Act*, *Spam Act* and the *Do Not Call Register Act*. These issues are discussed further in Chapter 64. The use of inconsistent definitions across federal, state and territory legislation that regulates personal information specifically is discussed in Chapters 4 and 14.

Proposal 12–1 The Australian Government and state and territory governments should ensure the consistency of definitions and key terms (for example, 'personal information', 'sensitive information' and 'health information') in federal, state and territory legislation that regulates the handling of personal information.

Freedom of Information Act 1982 (Cth)

12.10 The interrelationship between the FOI Act and the *Privacy Act* is significant. The FOI Act and the *Privacy Act* both regulate the way in which information is handled in government, but have different objectives. Freedom of information legislation is concerned mainly with transparency in government and protects privacy only to the extent that non-disclosure is, on balance, in the public interest. In contrast, privacy legislation is primarily focused on data protection and provides for transparency only to the extent that it enhances the information privacy rights of individuals.[7] The *Privacy Act* and the FOI Act are designed to interact with each other. For example, the public sector exemptions under the *Privacy Act* largely mirror the exemptions under the FOI Act.[8]

Disclosure of personal information

12.11 The most obvious interaction between the two Acts is that disclosing an individual's personal information to another person under the FOI Act has the potential to interfere with that individual's privacy. The FOI Act provides that every person has a legally enforceable right to obtain access to a document of an agency or an official document of a Minister, other than an exempt document.[9]

12.12 Section 41(1) of the FOI Act provides that a document is an exempt document if its disclosure under the Act would involve the unreasonable disclosure of personal

---

7 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [1.47].

8 See discussion in Ch 33.

9 *Freedom of Information Act 1982* (Cth) s 11.

information about any person (including a deceased person). The definition of 'personal information' in the FOI Act corresponds with that in the *Privacy Act*.[10] The exemption under s 41(1) is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own information.[11] It does not prevent reliance, however, on the exemption where the information cannot be separated from personal information about another person.[12]

12.13 The exemption under s 41 has been the subject of criticism and commentary.[13] In *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the ALRC and the Administrative Review Council (ARC) concluded that the provision should be amended to clarify the relationship between the FOI Act and the *Privacy Act*. To this end the review concluded that s 41 should be reworded to provide that a document is exempt if it contains personal information, the disclosure of which would constitute a breach of IPP 11; and the disclosure would not, on balance, be in the public interest.[14] The review also recommended that a Freedom of Information Commissioner[15] should issue guidelines to assist agencies to determine whether information is exempt under s 41.[16] These recommendations have not been implemented.[17]

Relationship with the 'Use and Disclosure' principle

12.14 In the ALRC's view, s 41 of the FOI Act should be amended to clarify the relationship between the FOI Act and the *Privacy Act*.[18] First, the section should provide that a document is exempt if it contains personal information and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle of the proposed Unified Privacy Principles (UPPs). The 'Use and Disclosure' principle provides the appropriate test of what constitutes a reasonable disclosure of personal information. This amendment will also clarify that a document

---

10 Ibid s 4. See Ch 3 for discussion of the definition of 'personal information' under the *Privacy Act*.

11 Ibid s 41(2).

12 See, eg, *Re Forrest and Department of Social Security* (1991) 23 ALD 131; M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [6.25].

13 See Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 10; Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001).

14 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.7] and Rec 59.

15 Ibid, [6.4] and Rec 18. See the discussion of a Freedom of Information Commissioner below.

16 Ibid, [10.8] and Rec 60.

17 See, however, the Freedom of Information Amendment (Open Government) Bill 2000 (Cth); Freedom of Information Amendment (Open Government) Bill 2003 [2004] (Cth); and Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001).

18 The ALRC did not receive any submissions on this issue.

cannot be withheld on privacy grounds where its disclosure is consistent with the 'Use and Disclosure' principle.[19]

12.15 In the FOI context there is, however, an additional dimension which is not reflected in the exceptions to the 'Use and Disclosure' principle—the public interest. The word 'unreasonable' in s 41 of the FOI Act incorporates a public interest test.[20] Whether disclosure is 'unreasonable' depends on whether the public interest factors that favour disclosure outweigh the privacy interests of the third party. To reflect this, s 41 should be amended to require an agency to consider whether, in respect of a particular document, disclosure would be in the public interest notwithstanding that disclosure would breach the 'Use and Disclosure' principle. This amendment will ensure the correct balance between the public interest in disclosure of a document and an individual's right to privacy.

12.16 The 'Use and Disclosure' principle includes an exception for uses and disclosures that are 'required or authorised by or under law'. If the 'required or authorised by or under law' exception applied in relation to s 41, it could be argued that any disclosure of personal information pursuant to the FOI Act would not be a breach of the 'Use and Disclosure' principle because disclosure under the FOI Act is authorised by or under law. In deciding, for the purposes of s 41, whether disclosure would constitute a breach of the 'Use and Disclosure' principle, this exception should be ignored insofar as it relates to release of information under the FOI Act. This will avoid any circularity that may otherwise arise from having a direct reference to the 'Use and Disclosure' principle in the section.[21]

Deceased individuals

12.17 Section 41 of the FOI Act provides that a document is an exempt document if its disclosure would involve the unreasonable disclosure of personal information about any person, including a deceased person. The proposed 'Use and Disclosure' principle includes an exception where an individual consents to a use or disclosure of his or her personal information. This exception will not be applicable in the case of deceased individuals.[22] Where none of the other exceptions to the 'Use and Disclosure' principle apply, this may give rise to a situation in which the personal information of a deceased individual cannot be disclosed. To ensure that information is not unreasonably

---

19 See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [6.24]. The Senate Legal and Constitutional Legislation Committee supported this amendment in Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.52].

20 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.7]. See, eg, *Albanese and Chief Executive Officer of the Australian Customs Service* [2006] AATA 900, [15]–[17], [22]–[34]; *Colakovski v Australian Telecommunications Corporation* (1991) 29 FCR 429.

21 See discussion in Ch 13.

22 The ALRC is not proposing that the *Privacy Act* be amended to provide for decisions to be made by third parties on behalf of deceased individuals. See discussion in Ch 3.

withheld in these circumstances, the ALRC proposes that where personal information is about a deceased individual, and the use or disclosure would otherwise require consent, an agency should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

Proposal 12–2 Section 41(1) of the *Freedom of Information Act 1982* (Cth) should be amended to provide that a document is exempt if it:

(a) contains personal information, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle and disclosure would not, on balance, be in the public interest; or

(b) contains personal information of a deceased individual, and the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle (but where the principle would require consent the agency must consider whether the proposed disclosure would involve the unreasonable disclosure of personal information about any individual including the deceased individual) and disclosure would not, on balance, be in the public interest.

Definition of 'personal information'

12.18 In Chapter 3, the ALRC proposes that the definition of 'personal information' should be amended to mean 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'. In the ALRC's view, the definition of 'personal information' should not be limited, as it currently is, to information about an individual who can be identified 'from the information'. For example, if an agency has access to other information and is able to link that information with information it holds in such a way that an individual can be identified, that individual is 'reasonably identifiable' and the information should be 'personal information' for the purposes of the *Privacy Act.* This amendment will bring the definition into line with other jurisdictions and international instruments.

12.19 The ALRC notes that s 41 of the FOI Act originally referred to information relating to a person's 'personal affairs'. It was amended in 1991, however, to bring its terminology into line with that used in the *Privacy Act* so that it now refers to 'personal information'.[23] The ALRC can see no reason why information about a 'reasonably identifiable individual' should not be protected under the FOI Act. The ALRC has therefore proposed that the definition of 'personal information' in the FOI Act should be amended to bring it into line with the ALRC's proposed definition.

23 *Freedom of Information Amendment Act 1991* (Cth) s 29.

Proposal 12–3 'Personal information' should be defined in the *Freedom of Information Act 1982* (Cth) as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

Guidelines

12.20 Agencies will still have to consider various factors on a case by case basis to determine whether a document falls within the exemption under s 41 of the FOI Act. In the ALRC's view, the body that is primarily responsible for administration of the FOI Act should issue guidelines to assist agencies to determine when information will be exempt under s 41. Until a Freedom of Information Commissioner is established, the body that is primarily responsible for administration of the *Freedom of Information Act 1982* (Cth) is the Attorney-General's Department.[24] The guidelines should incorporate guidance issued by the Privacy Commissioner on the proposed 'Use and Disclosure' principle.

12.21 The FOI Act also should require the body that is primarily responsible for administration of the FOI Act to consult the Privacy Commissioner when developing guidelines on s 41. The two bodies should liaise closely about relevant developments in this area and the guidelines should be reviewed whenever necessary.

Proposal 12–4 The *Freedom of Information Act 1982* (Cth) should be amended to require that the body that is primarily responsible for administration of the Act is to:

(a) develop and publish guidelines on the interpretation and application of s 41;

(b) consult with the Office of the Privacy Commissioner before issuing guidelines on the interpretation and application of s 41.

Required or authorised by or under law

12.22 An agency may decide to release personal information pursuant to a freedom of information request (FOI request) in some circumstances. The current Information Privacy Principle 11 (IPP 11) and the proposed 'Use and Disclosure' principle impose a general obligation on agencies not to disclose personal information to persons or organisations other than the individual concerned or his or her agent, unless one of the stated exceptions apply. A release of personal information pursuant to an FOI request is unlikely to breach IPP 11 or the proposed 'Use and Disclosure' principle, as it would

24 The role of a FOI Commissioner is discussed below.

be considered to be 'authorised' under law.[25] As noted in ALRC 77, however, the meaning of 'authorised' in this context is not clear.

> On one view, any release of information pursuant to a request made under the FOI Act is an 'authorised' release of information. On another view, the FOI Act does not 'authorise' the release of information because s 14 of the Act makes it quite clear that nothing in the Act prevents the release quite apart from the Act of information that can be properly released.[26]

12.23 In ALRC 77, the ALRC and the ARC recommended that the *Privacy Act* be clarified to provide that a release of personal information under the FOI Act constitutes a release that is 'required or authorised by law' for the purpose of IPP 11(1)(d).[27] This recommendation has not been implemented.

12.24 The ALRC considers that, in the interest of certainty, this issue should be clarified in the FOI Act. The ALRC therefore proposes that the FOI Act be amended to provide that disclosure of personal information in accordance with the FOI Act is a disclosure that is required or authorised for the purposes of the proposed 'Use and Disclosure' principle. In the ALRC's view, this will eliminate any possible confusion about the meaning of the exception as it relates to a release of information under the FOI Act.

12.25 The requirement that the disclosure of personal information be 'in accordance with the Act' would include that the consultation requirements under s 27A of the Act have been complied with. Section 27A of the FOI Act provides that an agency must consult with a third party before releasing his or her personal information if the agency determines that the person might reasonably wish to contend that the information is exempt and it is 'reasonably practicable' to consult with him or her. If an agency releases information pursuant to an FOI request without having regard to the provisions of the Act relating to consultation it would be open to the Privacy Commissioner to find that the agency had breached the 'Use and Disclosure' principle and to make a declaration, including that the complainant is entitled to compensation for any loss or damage suffered by reason of the information being released.

Proposal 12–5 The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act 1982* (Cth) is a disclosure that is required or authorised for the purposes of the proposed 'Use and Disclosure' principle under the *Privacy Act*.

---

25 *Privacy Act 1988* (Cth) s 14, IPP 11(1)(d). Australian Government Attorney-General's Department, *Freedom of Information Memorandum 93: FOI and the Privacy Act* (1992) states that disclosure required under the FOI Act comes within this exemption. See discussion in Ch 13 relating to provisions in federal legislation that require or authorise disclosure.

26 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.23].

27 Ibid, [10.23]–[10.24] and Rec 65.

Access and correction

12.26 Both the FOI Act and the *Privacy Act* enable individuals to access their own personal information and to amend or annotate that information if it is incorrect, incomplete, out-of-date or misleading. The rights provided by the *Privacy Act* are found in IPP 6 and IPP 7. The amendment rights in the FOI Act are located in Part V and are dependent on a person having previously obtained lawful access under the Act to the relevant documents. Persons who fail to satisfy this requirement must use the procedures provided in the *Privacy Act*.[28]

12.27 Part V was included in the FOI Act before the introduction of the *Privacy Act*. In 1987, the Senate Standing Committee on Legal and Constitutional Affairs recommended that the amendment provisions be transferred from the FOI Act to privacy legislation 'should the latter be enacted'.[29] This did not happen when the *Privacy Act* was enacted in 1988.

12.28 The *Privacy Act* includes provisions to ensure that the access and amendment provisions under both Acts interact with each other.[30] The OPC has stated that as a result of the terms of IPPs 6 and 7, read in conjunction with s 34 of the *Privacy Act*, it will generally decline to investigate a complaint about access or amendment of public sector information if the complainant has not exhausted all FOI Act processes.[31] The OPC noted that this can result in complainant dissatisfaction and confusion, and unnecessary administrative costs and processes. Since 2001, the OPC has declined 17 complaints about access and seven complaints about amendment.[32]

12.29 Under IPP 7 an applicant may apply for amendment of personal information on the grounds that it is inaccurate or, given its purpose, irrelevant, misleading, incomplete or not up-to-date. The FOI Act does not include a reference to 'purpose'.[33] Further, the right to amend personal information under IPP 7 is broader than the corresponding right in the FOI Act. An application for amendment will need to be dealt with under the *Privacy Act* rather than the FOI Act where the amendment sought is on

---

28 *Privacy Act 1988* (Cth) s 35.

29 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Freedom of Information Act 1982—The Operation and Administration of the Freedom of Information Legislation* (1987), [15.7].

30 See, eg, *Privacy Act 1988* (Cth) s 34.

31 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; *S v Various Commonwealth Agencies* [2004] PrivCmrA 8; Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 13. Section 34 prohibits the Privacy Commissioner from providing certain information about documents if they would be exempt documents under *Freedom of Information Act 1982* (Cth).

32 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. The OPC has declined these complaints under s 41(1)(f) of the *Privacy Act* on the grounds that the complaint would best be dealt with under another law.

33 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.17].

the grounds that the information is irrelevant; where a person seeks deletion of personal information; or where a person seeks amendment of personal information in a record to which he or she has not been provided lawful access.[34]

12.30 An application to access and amend a document under the *Privacy Act* cannot be made before the period to appeal a decision made under the FOI Act to the Federal Court has expired or such an appeal has been determined.[35] Under the FOI Act, however, a person may also seek review by the Administrative Appeals Tribunal (AAT) of an agency's decision under the Act not to grant access and amendment of personal information.[36]

Submissions and consultations

12.31 In IP 31, the ALRC asked whether the overlap of the *Privacy Act* and FOI Act provisions relating to access and amendment of records gives rise to any difficulties.[37]

12.32 A number of stakeholders submitted that the overlap has created confusion for both agencies and the public.[38] It was argued in some submissions that access and amendment should continue to be provided primarily under the FOI Act.[39] The Governments of Victoria and Queensland noted that access and amendment rights are generally exercised under freedom of information legislation in their jurisdictions.[40] The Government of Victoria noted that:

> FOI laws would need to be retained under any harmonised scheme. That being so, it is on the whole simpler for those bodies to continue to apply FOI laws to requests by individuals for their personal or health information—that is, to maintain one statutory process for all access requests. This is the reason for the Victorian provisions, and it is suggested that this approach ought to be retained.[41]

12.33 The Office of the Information Commissioner Northern Territory stated that the FOI Act has an advantage because it deals with procedural matters in detail. The Office suggested that:

---

34 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 18. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.23]–[4.24].

35 *Privacy Act 1988* (Cth) s 35.

36 *Freedom of Information Act 1982* (Cth) s 55.

37 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7-6(a).

38 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; D Hall, *Submission PR 61,* 27 November 2006.

39 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Confidential, *Submission PR 165,* 1 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

40 Government of Victoria, *Submission PR 288,* 26 April 2007; Queensland Government, *Submission PR 242,* 15 March 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

41 Government of Victoria, *Submission PR 288,* 26 April 2007.

> One approach to avoid duplication would be to state in the privacy principles that requests for access or amendment in respect of government agencies must be made under the FOI Act to the extent that there is power to deal with the issues under that Act.[42]

12.34 The Office of the Information Commissioner Northern Territory also submitted, however, that there may be some argument for removing the amendment provisions from the FOI Act as they sit naturally within the realm of privacy protection, while the access provisions are based on much broader considerations. The Office also noted that simply deleting or transferring the FOI access provisions would not be an ideal solution because FOI access applications are frequently made up of a mix of personal and non-personal information. An applicant in this situation would therefore have to make two applications.[43]

12.35 The OPC and the Commonwealth Ombudsman submitted that there is an argument that IPP 6 and IPP 7 should be allowed to work to the full, rather than having their practical operation limited by the FOI Act.[44] The OPC noted that it may be contrary to the spirit of the *Privacy Act*, and inconsistent with the rights of access under NPP 6, if IPP 6 and IPP 7 continue to be subject to the FOI Act. The OPC suggested that it would be unnecessary to subject individuals to the FOI Act process, which is primarily designed for accessing the deliberative process of government, if a simpler process could be facilitated under the *Privacy Act*.

> Accordingly, the Office suggests that IPPs 6 and 7 could be amended to provide a further mechanism by which individuals can seek access to and correction of their personal information held by Australian and ACT government agencies, in addition to the FOI Act process. This would not mean creating provisions that are inconsistent with the FOI Act. Rather, it may involve amending the IPPs to require agencies to give access, subject to particular exceptions listed under IPP 6 (including relevant exemptions currently found in the FOI Act). This may also need to be considered if a single set of privacy principles were adopted.[45]

ALRC's view: Access and correction to be dealt with in the Privacy Act

12.36 In ALRC 77, the ALRC and the ARC considered the overlap of the *Privacy Act* and FOI Act provisions relating to access and amendment of records, and concluded that it did not give rise to any major difficulties.[46] Submissions to this Inquiry have noted, however, that the overlap can lead to confusion for agencies and the public.

---

42 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

43 Ibid.

44 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007. See Commonwealth Ombudsman, *Scrutinising Government: Administration of the Freedom of Information Act 1982 in Australian Government Agencies*, Report No 2 (2006), [4.14]–[4.15]; [7.5], [8.2].

45 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

46 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.17].

12.37 The ALRC has considered various models for dealing with the overlap, including having access and amendment dealt with exclusively under the FOI Act. Some of the exemption categories in the FOI Act are broad, however, and are based on policy considerations other than privacy. Further, the access procedures under the FOI Act can be cumbersome. The Attorney-General's Department recently reported that 62% of requests for amendment of personal records took over 60 days to process.[47] It is the ALRC's view that individuals should have access to a simple and user-friendly process to access and correct their own personal information.

12.38 Another option is for access to personal information to be dealt with under the FOI Act, and amendment under the *Privacy Act*. In the ALRC's view, however, it would be confusing for agencies and the public to have access and amendment dealt with under more than one Act.

12.39 In the ALRC's view, an individual's right to access or amend his or her own personal information held by an agency should be dealt with under a new Part in the *Privacy Act*. The right to access and amend one's own personal information are fundamental privacy rights[48] and should be dealt with under privacy legislation and subject to oversight by the Privacy Commissioner. The ALRC notes that the majority of applications for access under the FOI Act relate to access to personal information. The *Freedom of Information Annual Report* states that in 2005–06, 85% of the 41,430 FOI requests received that year were for documents containing personal information. It is not clear from the report what percentage of these requests were from individuals seeking access to their own personal information. The remaining 15% of FOI requests were for documents concerning policy development and government decision making. The Report also notes that, in 2005–06, 1,414 FOI requests related to the amendment of personal records.[49]

12.40 The ALRC notes that the heading in IPP 7 refers to 'alteration', and Part V of the FOI Act refers to 'amendment' of personal information. NPP 6 and the proposed 'Access and Correction' principle, however, refer in the heading to 'correction' of personal information. In the interest of consistency with the proposed 'Access and Correction' principle, the new Part should refer to 'correction', rather than 'amendment'.[50]

---

47 Australian Government Attorney-General's Department, *Freedom of Information Annual Report 2005–2006* (2006), [1.32].

48 See, eg, European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998. See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12.

49 A request for personal information means a request for documents which contain information about a person: Australian Government Attorney-General's Department, *Freedom of Information Annual Report 2005–2006* (2006), [1.7]–[1.31].

50 For this reason, the rest of this section refers to 'correction' rather than 'amendment' of personal information.

12.41 The Office of the Information Commissioner Northern Territory submitted that FOI access applications are frequently made up of a mix of personal and non-personal information.[51] In the ALRC's view, this issue can be dealt with administratively by agencies and the AAT, for example, by designing forms to allow for applications relating to personal and non-personal information to be dealt with together.

12.42 In the interest of clarity, the ALRC proposes that the FOI Act be amended to provide that an individual's right to access or correct his or her own personal information is dealt with under the *Privacy Act*, and that Part V of the FOI Act should be repealed.

Proposal 12–6 The *Privacy Act* should be amended to provide a new Part dealing with access to, and correction of, personal information held by an agency.

Proposal 12–7 The *Freedom of Information Act 1982* (Cth) should be amended to:

(a) provide that an individual's right to access or correct his or her own personal information is dealt with under the *Privacy Act*; and

(b) repeal Part V of the Act.

ALRC's view: access

12.43 One issue is that, while the FOI Act[52] and IPP 6 provide a *right* for an individual to access personal information about him or her, NPP 6 and the proposed 'Access and Correction' principle create an obligation for organisations to provide access to personal information. The ALRC has not formed a strong view as to whether the provision dealing with access in the proposed Part dealing with access and correction of personal information held by agencies should be expressed as a right of an individual or an obligation of an agency. In the interest of consistency with the proposed 'Access and Correction' principle, however, the ALRC has proposed that the provision should be expressed as an obligation.

Advice that correction may be made

12.44 There is currently no obligation under the *Privacy Act* or the FOI Act to advise an individual that he or she may request the correction of his or her personal information where that individual has been given access to that information. Such an obligation exists under Information Privacy Principle 6 of the *Privacy Act 1993* (NZ). In the ALRC's view, it is appropriate that agencies should inform individuals of their

51 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
52 *Freedom of Information Act 1982* (Cth) s 11.

right to seek correction of their personal information where that individual has been given access to that information.

Use of a mutually agreed intermediary

12.45 NPP 6.3 requires an organisation to consider whether, instead of refusing access, a compromise can be reached using a mutually agreed intermediary that would allow an individual some form of indirect access to his or her personal information, provided that such access serves the needs of both parties. In Chapter 26, the ALRC proposes that the proposed 'Access and Correction' principle provide that an organisation should take reasonable steps to reach a compromise that adequately meets the needs of both parties.[53] In the ALRC's view, this provision could be useful in the context of providing access to personal information held by an agency. It allows for a more flexible response, and balances the need to withhold access to personal information in appropriate circumstances with an individual's right to know what personal information is held about him or her.

Access other than under the Privacy Act

12.46 Section 14 of the FOI Act currently provides that:

> Nothing in this Act is intended to prevent or discourage Ministers and agencies from publishing or giving access to documents (including exempt documents), otherwise than as required by this Act, where they can properly do so or are required by law to do so.

12.47 It is the ALRC's view that this provision should be mirrored in the *Privacy Act*. Where appropriate, agencies should be able to provide an individual with access to their own personal information outside of the process outlined in the proposed Part dealing with access to, and correction of, personal information held by an agency.

Proposal 12–8 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that:

(a) if an agency holds personal information about an individual the agency must, if requested by the individual, provide the individual with access to the information, subject to a number of exceptions under the Part;

(b) where an individual is given access to personal information, the individual must be advised that he or she may request the correction of that information;

(c) where an agency is not required to provide the individual with access to personal information because of an exception, the agency must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties; and

53 See Proposal 26–2.

(d) nothing in the Part is intended to prevent or discourage agencies from publishing or giving access to personal information, otherwise than as required by the Part, where they can do so properly or are required to do so by law.

Exceptions

12.48 IPP 6 provides individuals with a right to access a record that contains personal information about them 'except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents'.[54] The effect of this provision is to subject the right to access personal information under the *Privacy Act* to the exemptions under the FOI Act.

12.49 A number of the exemptions under the FOI Act would clearly need to be reproduced in the proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency. These exemptions would include, for example, the exemptions relating to documents affecting national security, defence or international relations; documents affecting relations with states; Cabinet documents; Executive Council documents; documents affecting enforcement of law and protection of public safety; and documents subject to legal professional privilege.[55] Other exemptions, however, such as the 'internal working documents' exemption and 'documents concerning certain operations of agencies' may not be appropriate in the privacy context.[56] The ALRC is interested in stakeholder views on what exceptions should apply to the general provision granting an individual the right to access his or her own personal information.

Question 12–1 What exceptions should apply to the general provision granting an individual the right to access his or her own personal information held by an agency? For example, should the exceptions mirror the provisions in Part IV of the *Freedom of Information Act 1982* (Cth) or should another set of exceptions apply?

ALRC's view: correction

12.50 As noted above in relation to access, the ALRC has not formed a strong view on whether the provision dealing with correction in the proposed Part of the *Privacy Act* should be expressed as a right or an obligation. It is the ALRC's preliminary view,

54 *Privacy Act 1988* (Cth) s 14, IPP 6.
55 *Freedom of Information Act 1982* (Cth) ss 33, 33A, 34, 35, 37.
56 Ibid ss 36, 40.

however, is that in the interest of consistency with the proposed 'Access and Correction' principle, the provision should be expressed as an obligation.

12.51 The provision dealing with correction in the proposed Part of the *Privacy Act* maintains the same obligations that are provided for under IPP 7. For example, the provision retains the requirement that an agency take reasonable steps to ensure that personal information is relevant, up-to-date, complete and not misleading, having regard to the purpose for which the information was collected, or is to be used, and to any purpose that is directly related to that purpose. Further, IPP 7 and the FOI Act both provide for the annotation of a record following an unsuccessful application for correction.[57] In the ALRC's view, this requirement should be available under the Part dealing with access and correction of personal information held by agencies.

Lawful access before correction

12.52 One submission noted that, under IPP 7.2, where a person's record is exempt from access because of an exemption under the *Privacy Act* or the FOI Act, the data subject has no right to insist on correction if they find out by informal means, or reasonably suspect, that the non-accessible record is incorrect. It was submitted that this is an unsatisfactory state of affairs, which could be dealt with by ensuring the *Privacy Act* right of correction is not conditional on the right of access.[58] It was submitted that:

> Correction obligations should apply independently of rights of access—i.e. the right of individuals to seek correction should apply whether they have obtained access through formal processes (such as under the *Privacy* or FOI Acts) or have become aware of the information by other means.[59]

12.53 In the ALRC's view, IPP 7.2 does not require lawful access before an individual can seek correction of their own personal information.[60] Lawful access is, however, a requirement under s 48 of the FOI Act. In ALRC 77, the ALRC and ARC recommended that the requirement of lawful access should be removed from the FOI Act.[61] The ALRC noted that:

> Access as a prerequisite to seeking amendment or annotation under the FOI Act arises from the fact that amendment rights were first introduced in the FOI Act which deals primarily with access and were regarded as complementary to the right of access. It has been presumed that the only way an individual would know that information was

---

57 *Privacy Act 1988* (Cth) s 14, IPP 7.3; *Freedom of Information Act 1982* (Cth) s 51.

58 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

59 Ibid.

60 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 18. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.23]–[4.24].

61 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 77.

> incomplete, incorrect, out of date or misleading would be if they had access to the document.[62]

12.54 The Freedom of Information (Open Government) Bill 2000 (Cth) included an amendment to remove the requirement for lawful access to amend and annotate records under the FOI Act. The Senate Legal and Constitutional Legislation Committee did not support this amendment.[63]

12.55 In the ALRC's view, the provision dealing with correction of personal information in the proposed Part of the *Privacy Act* should not provide that lawful access is a prerequisite to the correction of personal information. There may be situations in which a person is legitimately denied access to a document because it is exempt, but they are sufficiently aware of the contents of the document to know or suspect that it contains false information. The ALRC also notes that lawful access is not a requirement before exercising the rectification right under art 12(b) of the European Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[64]

Correction by amendment, deletion or annotation

12.56 The OPC submitted that, in the interests of consistency, and in the spirit of both the *Privacy Act* and the FOI Act, it may also be appropriate to expand the amendment rights under the FOI Act to align with those currently under IPP 7.[65] In the ALRC's view, the proposed Part of the *Privacy Act* dealing with access and correction of personal information held by agencies should include the same obligations to make corrections, additions and deletions as are available under IPP 7. The ALRC notes that, in ALRC 77, it recommended that the FOI Act be amended to bring it in line with the *Privacy Act* in this regard.[66]

Making corrections and annotations available to subsequent users

12.57 In Chapter 26, the ALRC proposes that the 'Access and Correction' principle that relates to organisations should provide that, where an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed before correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances. This requirement should also apply to agencies.

---

62 Ibid, [12.9].

63 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.69].

64 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

65 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

66 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 79.

12.58 One submission noted that the the *Privacy Act* should specify that an annotation should be made available to any subsequent user of the disputed personal information.[67] Information Privacy Principle 7(3) of the *Privacy Act 1993* (NZ) provides that where an agency has corrected or annotated personal information the agency shall, if reasonably practicable, inform each person, body or agency to whom the personal information has been disclosed of those steps. The ALRC does not propose that organisations should be obliged to ensure that an annotation is available to any subsequent user of the personal information. In the ALRC's view, this obligation is implicit in the requirement for an agency to take reasonable steps to annotate, on request, personal information.

Proposal 12–9 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that, if an agency holds personal information about an individual, the agency must:

(a) if requested by the individual, take such steps to correct (by way of making appropriate corrections, deletions or additions) the information as are, in the circumstances, reasonable to ensure that the information is, with reference to a purpose of collection permitted by the proposed Unified Privacy Principles, accurate, complete, up-to-date, relevant and not misleading;

(b) where the agency has taken the steps outlined in (a) above, if requested to do so by the individual, and provided such notification would be practicable in the circumstances, notify any other entities to whom the personal information has already been disclosed.

Proposal 12–10 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that where an agency decides not to correct the personal information of an individual, and the individual requests the agency to annotate the personal information with a statement by the individual claiming that the information is not accurate, complete, up-to-date, relevant, or is misleading, the agency must take reasonable steps to do so.

ALRC's view: procedure for providing access to, and correction of, personal information

12.59 The proposed Part of the *Privacy Act* dealing with access and correction should set out a procedure for an individual to apply to access and correct their own personal information. In the ALRC's view, this procedure should be similar to, but less onerous than, the process set out in the FOI Act.

---

67 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

12.60 The procedure should address a number of matters that are currently provided for under the FOI Act. These matters include: requirements for making an application for correction or annotation of personal information; time periods for processing a request to access or correct personal information; and the transfer of a request to access or correct personal information to another agency in certain circumstances (for example, when a document is not in the possession of an agency but is, to the knowledge of that agency, in the possession of another agency).

12.61 The Part should also set out: how personal information is to be made available to the individual (including by giving the individual a reasonable opportunity to inspect the records, or by providing a copy of the record, by giving a summary of the contents of the record, by providing oral information about the contents of the record); the deletion of exempted matter or irrelevant material; when a request for access to personal information may be refused by an agency (for example, when it would substantially and unreasonably divert the resources of the agency from its other operations, or in the case of a minister, would substantially and unreasonably interfere with the performance of the minister's functions); and how reasons for a decision to deny a request to access or correct personal information are to be provided.

Proposal 12–11 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should set out a process for dealing with a request to access or correct personal information that addresses:

(a) the requirements for making an application for correction or annotation of personal information;

(b) time periods for processing a request to access or correct personal information;

(c) the transfer of a request to access or correct personal information to another agency in certain circumstances (for example, when a document is not in the possession of an agency but is, to the knowledge of that agency, in the possession of another agency);

(d) how personal information is to be made available to the individual (including by giving the individual a reasonable opportunity to inspect the records, or by providing a copy of the record, by giving a summary of the contents of the record, or by providing oral information about the contents of the record);

(e) how corrections are to be made (including by additions and deletions);

(f) the deletion of excepted matter or irrelevant material;

(g) the persons authorised to make a decision on behalf of an agency in relation to a request to access or correct personal information;

(h) when a request for access to personal information may be refused by an agency (for example, when it would substantially and unreasonably divert the resources of the agency from its other operations, or in the case of a minister, would substantially and unreasonably interfere with the performance of the minister's functions); and

(i) the provision of reasons for a decision to deny a request to access or correct personal information.

ALRC's view: review and complaints

12.62 The ALRC notes the OPC's comments that it will generally decline to investigate a complaint about access to, and correction of, personal information held by an agency if the complainant has not exhausted all FOI Act processes. An applicant will have to access the FOI Act process and then complain to the Privacy Commissioner if an applicant wishes to seek: correction on the grounds that the information is irrelevant; deletion of personal information; or correction of personal information in a record to which he or she has not been provided lawful access.

12.63 The ALRC also notes that, while the Privacy Commissioner has the power to order compensation under the *Privacy Act*,[68] the AAT does not have this power under the FOI Act. If an applicant wants compensation for a failure by an agency to provide access to, or correction of, personal information, the applicant will have to use the FOI Act to access and correct the personal information, and then the *Privacy Act* process to seek compensation.

12.64 The ALRC acknowledges that this process is necessary because of the interaction between the *Privacy Act* and the FOI Act. In the ALRC's view, however, this process is deficient and needlessly cumbersome. The proposed Part dealing with access to, and correction of, personal information held by agencies should provide for a simplified review and complaints mechanism.

12.65 In the ALRC's view, the Part should provide for the same review rights and complaints mechanism as under the FOI Act—internal review by an agency and review by the AAT.[69] The Part should also provide for a complaint to be made to the Commonwealth Ombudsman. The ALRC notes the extensive experience of the AAT and the Commonwealth Ombudsman in relation to access to, and correction of, personal information,and the operation of the exemptions under the FOI Act.

12.66 The Part should provide that the AAT may make an order for compensation for any loss or damage suffered as a result of the agency's decision not to grant access to, or correction of, personal information. The ALRC acknowledges that it is unusual to have the AAT make a primary decision in relation to compensation. The ALRC notes,

---

68 *Privacy Act 1988* (Cth) s 52.

69 Decisions of the AAT are reviewable by the Federal Court of Australia: *Administrative Appeals Tribunal Act 1975* (Cth) pt IVA.

however, that the AAT currently has the power under s 105.51(7)(b) of the *Criminal Code* (Cth) to compensate a person for his or her detention when the AAT has found a decision to make a preventative detention is void. The ALRC also notes the constitutional limits in relation to this power.[70]

12.67 The Privacy Commissioner should have an oversight and educational role in relation to access and correction. The *Privacy Act* currently provides for the Privacy Commissioner to have a number of oversight and education functions that would allow the Commissioner to undertake this role.[71] The Commissioner's oversight functions provide important tools to increase understanding of federal privacy law among individuals and agencies, and enable the Commissioner to be proactive in preventing non-compliance. In the ALRC's view this education and oversight role should include issuing guidelines on access to, and correction of, records containing personal information held by an agency.

Proposal 12–12 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide for:

(a) internal review by an agency of a decision made under the Part;

(b) review by the Administrative Appeals Tribunal of a decision made under the Part (including the power to make an order for compensation); and

(c) complaints to the Commonwealth Ombudsman.

Proposal 12–13 The Office of the Privacy Commissioner should issue guidelines on access to, and correction of, records containing personal information held by an agency.

An exemption for complaint-handling files

12.68 The OPC submitted that the ALRC may wish to consider whether the Office's complaints files should be exempt from disclosure under the FOI Act. The OPC noted that such complaints deal with the issue of privacy itself, and that the Office of the NSW Privacy Commissioner's complaint-handling, investigative and reporting functions are exempt under the *Freedom of Information Act 1989* (NSW).[72]

12.69 The OPC noted that it is currently possible under the FOI Act to exempt, on a case by case basis, documents that may unreasonably disclose personal information.[73] The OPC submitted, however, that a 'cover-all' exemption would be consistent with

70 See discussion of *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245 in Ch 43.
71 *Privacy Act 1988* (Cth) s 27(1)(d), 27(1)(m).
72 See, eg, *Freedom of Information Act 1989* (NSW) s 9 and sch 2.
73 *Freedom of Information Act 1982* (Cth) s 41(1).

public expectations of privacy, heighten the trust of complainants, and reinforce the OPC's commitment to leadership in good privacy practice.[74] The ALRC is interested in views on whether the complaint-handling, investigative and reporting functions of the OPC should be exempt under the FOI Act.

Question 12–2 Should the Office of the Privacy Commissioner's complaint-handling, investigative and reporting functions be exempt under the *Freedom of Information Act 1982* (Cth)?

Archives Act 1983 (Cth)

12.70 The *Archives Act 1983* (Cth) establishes the National Archives of Australia (National Archives) and provides for the preservation of the archival resources of the Commonwealth. It also creates an access regime whereby the public generally has a right of access to Commonwealth records that are more than 30 years old (the open access period).[75] The *Archives Act* provides some protection for information relating to the personal affairs of any person (including a deceased person).[76]

12.71 The *Privacy Act* provides that records containing personal information in the custody of the National Archives are subject to the operation of the *Privacy Act*. Two exceptions apply: when the records are in the open access period or where records are subject to arrangements with a person other than a Commonwealth institution providing for the extent to which the National Archives or other persons are to have access to them.[77] The *Archives Act* controls access to these categories of records.

12.72 While NPP 4 provides that an organisation must take reasonable steps to destroy or permanently de-identify personal information after a certain amount of time, there is no equivalent IPP to govern the retention of records by agencies.[78] Instead, the *Archives Act* regulates the retention of records. It prohibits the destruction of Commonwealth records without the permission of National Archives, subject to some exceptions.[79]

The 'personal affairs' exemption

12.73 Section 33(1)(g) of the *Archives Act* provides an exception to public access to records if the access would involve the unreasonable disclosure of information relating to the 'personal affairs of any person (including a deceased person)'. This is in contrast to s 41 of the FOI Act, which currently exempts a document if disclosure 'would

74 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
75 *Archives Act 1983* (Cth) s 31.
76 Ibid s 33. See discussion below.
77 See the definition of 'record' in *Privacy Act 1988* (Cth) ss 6. The second exception would relate to, eg, arrangements between individuals to have their personal collections held by National Archives, for example, the 'Whitlam collection' or the 'Fraser collection'.
78 See discussion in Ch 25.
79 See *Archives Act 1983* (Cth) ss 24–29.

involve the unreasonable disclosure of personal information about any person (including a deceased person)'.[80]

12.74 'Personal affairs' is generally considered to be a narrower concept than 'personal information'. In *Young v Wicks*, 'personal affairs' was interpreted as 'matters of private concern to a person'.[81] In *Colakovski v Australian Telecommunications Corporation*, however, the Federal Court held that the phrase was not confined to 'affairs that are private in the sense of secret to the person'.[82] Other interpretations of 'personal affairs' include 'the composite collection of activities personal to the individual concerned',[83] and that the term includes 'private behaviour, home life and personal family relationships'.[84]

12.75 What is critical to the definition of 'personal information' under the *Privacy Act*, however, is that information is capable of identifying an individual rather than its specific nature. Under the current definition of 'personal information',[85] if a person's identity is clear, or reasonably capable of being ascertained, then any information about them is covered, whether or not it is sensitive.[86]

Submissions and consultations

12.76 In IP 31, the ALRC asked whether s 33(1)(g) of the *Archives Act* should be amended to provide an exemption in relation to 'personal information' as defined in the *Privacy Act*. The ALRC received only a few submissions on this issue.

12.77 The OPC noted that the exemption could result in the unreasonable disclosure of personal information when that information does not meet the criteria of 'personal affairs'. The OPC submitted that amending the 'personal affairs' exemption to apply to 'personal information' would protect privacy better, and harmonise the *Archives Act* with both the *Privacy Act* and the FOI Act.[87] In the OPC's view

> changing the exemption would not defeat the public interest of allowing access to the national archives. Rather, it would provide greater scope to fairly consider whether a disclosure would be 'unreasonable' in the circumstances, and prevent the disclosure of personal information in circumstances that would otherwise be a breach of the IPPs.[88]

---

80 See discussion of *Freedom of Information Act 1982* (Cth) s 41 above.
81 *Young v Wicks* (1986) 13 FCR 85, 89.
82 *Colakovski v Australian Telecommunications Corporation* (1991) 29 FCR 429, 436.
83 *Commissioner of Police v District Court of New South Wales* (1993) 31 NSWLR 606, 625.
84 *Re F and Health Department* (1988) 2 VAR 458, 461.
85 *Privacy Act 1988* (Cth) s 6(1).
86 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005).
87 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Confidential, *Submission PR 143,* 24 January 2007.
88 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

12.78 There was strong opposition to such an amendment from other stakeholders.[89] The National Archives noted that it had considered this issue and argued against the change when it was raised in the ALRC's review of the *Archives Act*.[90]

> Advice we received at the time was that 'personal information' is much wider than the meaning attributed to 'personal affairs' and a vast range of information about individuals which currently does not come within the definition of personal affairs would need to be considered for exemption if this change was made. It would in practice unnecessarily restrict access to records, undermining the intent of the *Archives Act*. In addition it would vastly increase the workload of decision-makers under the *Archives Act*.[91]

12.79 National Archives argued that the lack of uniformity with the FOI Act terminology has not caused any difficulty in the application of the *Archives Act* or FOI Act to date and is a sensible recognition of the different age of the information covered by the two pieces of legislation. National Archives stated that:

> 'personal affairs' is an appropriate description of the sort of information that needs to be exempted in archival records. While the release of much 'personal information' could not be argued to be unreasonable after 30 years, 'personal affairs' enables the exemption of information which is likely to retain sensitivity, i.e. information about family, marital, domestic and sexual relationships, health, adoption, illegitimacy, infidelity, etc.[92]

12.80 The Australian Privacy Foundation opposed any change to the exemption and claimed that the amendment of s 41 of the FOI Act from 'personal affairs' to 'personal information' has had the consequence of allowing agencies to claim the personal information exemption more often, in circumstances where the information in question is about the official business role of public servants.

> This has reduced accountability and discredits the privacy protection in the eyes of the public and the media. There may be a case for reintroducing a clear distinction between personal information and personal affairs in the context of disclosure limitations, while ensuring that individuals obtain the benefit of the wider definition in the context of other rights.[93]

ALRC's view

12.81 The ALRC does not make any proposal in relation to the 'personal affairs' exemption under the *Archives Act*. This position contrasts with that taken by the ALRC in *Australia's Federal Record: A Review of the Archives Act 1982* (ALRC 85). The ALRC's view, however, is that in the absence of any identifiable problem in this area,

---

89 Queensland Government, *Submission PR 242,* 15 March 2007; National Archives of Australia, *Submission PR 199,* 20 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

90 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998).

91 National Archives of Australia, *Submission PR 199,* 20 February 2007.

92 Ibid.

93 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

the benefits in changing the exemption to refer to 'personal information' do not outweigh the disadvantages of such an amendment.

12.82 Strong arguments were put forward in submissions that opposed any change to the exemption. The ALRC is concerned that changing the exemption to refer to 'personal information' may have the affect of needlessly restricting access to records, and undermine the intent of the *Archives Act*. The ALRC is also conscious that such a change would increase the workload of decision makers under the *Archives Act*. The lack of uniformity with the FOI Act terminology has not caused any difficulty in the application of the *Archives Act* and FOI Act to date, and is an appropriate recognition of the different age and sensitivity of the information covered by the Acts.

The open access period

12.83 In IP 31, the ALRC asked whether the *Privacy Act* should apply to certain classes of records in the open access period for the purposes of the *Archives Act*. The OPC submitted that:

> there are instances where the protections under the *Archives Act* have not appeared to meet with individuals' expectations as to how their personal information will be protected. For example, the Office is aware of a case where an open access Commonwealth record, containing medical information, remained publicly accessible for some time. In this case, the individual and the NAA differed in their views as to whether the information might cause social stigma or be sensitive.[94]

12.84 The OPC suggested that one option would be to subject Commonwealth records in the open access period to coverage by IPP 11. Alternatively, the *Archives Act* could mirror the provisions of IPP 11. If exemptions that prevent disclosure under the *Archives Act* can afford an appropriate standard of protection, however, then extending the coverage of the *Privacy Act* may not be necessary.[95]

12.85 This view was opposed strongly in submissions from federal and state public records authorities.[96] National Archives argued that the exclusion of records in the open access period from the coverage of the *Privacy Act* is a recognition that the sensitivity of much personal information has diminished after 30 years.

> Decisions to release or restrict Commonwealth records from the public under the *Archives Act* are made by the National Archives, providing a safeguard against possible self-interest on the part of government agencies in inappropriately restricting access to information. These are important and valuable principles which should be preserved and which stand apart from the question of national consistency in the

94 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
95 Ibid.
96 Queensland Government, *Submission PR 242,* 15 March 2007; National Archives of Australia, *Submission PR 199,* 20 February 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

> regulation of personal information, particularly if the latter increases costs and complicates the bureaucratic process.[97]

12.86 National Archives noted that extending the coverage of the *Privacy Act* to Commonwealth records in the open access period would limit public access to records, and would impose an unworkable burden on the administration of access by National Archives. The National Archives noted that it withholds information that retains sensitivity beyond the 30 year closed period.[98]

ALRC's view

12.87 The ALRC considered this issue in ALRC 85 and concluded that the application of the IPPs to records more than 30 years old would be needlessly restrictive. The ALRC stated that the exemption categories within the archives legislation continue to provide appropriate protection for personal information.[99]

12.88 The ALRC affirms that view. The access regime in the open access period must take into consideration the fact that sensitivities attaching to information may diminish after 30 years. Prohibiting the disclosure of all personal information, including names of individuals, would greatly restrict access to archival records. This does not mean, however, that privacy should be disregarded when making access decisions. Exemption categories within the archives legislation must include appropriate protection for personal information. In the ALRC's view, the proposed exemption in relation to 'personal information', and the guidelines developed in consultation with the OPC, will be sufficient to deal with this.

12.89 The open access period in each state and territory varies. For example, under the *Territory Records Act 2002* (ACT) a record of an agency is open to public access if 20 years has elapsed since the record came into existence. Under the federal *Archives Act, State Records Act 1998* (NSW) and the *Public Records Act 1973* (Vic), the open access period is 30 years, and under the *Archives Act 1983* (Tas) it is 25 years.[100] In the ALRC's view, in the interest of national consistency, the Australian Government and state and territory governments, in consultation with the Council of Australasian Archives and Records Authorities should consider reviewing the *Archives Act* and equivalent state and territory public records legislation to ensure that the 'open access period' under each Act is consistent.

A single information Act?

12.90 One option for consideration is whether, given the significant overlap between the FOI Act and the *Privacy Act*, the two Acts should be consolidated into a single Act. A number of overseas jurisdictions have combined freedom of information and privacy

---

97 National Archives of Australia, *Submission PR 199,* 20 February 2007.

98 Ibid.

99 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), [15.56].

100 See, eg, *Archives Act 1983* (Cth) s 31; *State Records Act 1989* (NSW) s 26; *Public Records Act 1973* (Vic) s 10; *Archives Act 1983* (Tas) s 15.

legislation.[101] The ALRC and the ARC considered this option in ALRC 77. The proposal was rejected on the basis that there was insufficient benefit in the proposal to outweigh the disadvantage in disturbing the existing legislative framework.[102]

12.91 Another option is to consolidate the FOI Act, the *Privacy Act* and the *Archives Act* into a single Act. An example of such an Act is the *Information Act 2002* (NT). The ALRC and the ARC also considered this option in ALRC 77. It was thought that this consolidation would address the overlap between the *Privacy Act* and FOI Act and bring together the major provisions dealing with access to government held information and records management. The option met with strong opposition in submissions to the ALRC and ARC review of the FOI Act and was ultimately rejected. The ALRC and ARC recommended, however, that the *Privacy Act*, FOI Act and *Archives Act* should be amended, where necessary, to provide a cohesive and consistent package of legislation on government records.[103]

Submissions and consultations

12.92 There was little support for combining the *Privacy Act*, FOI Act and *Archives Act*. Stakeholders noted that the three Acts have different purposes, and considered that the ALRC should focus on the harmonisation of the Acts.[104]

12.93 The Office of the Information Commissioner Northern Territory submitted that there is significant merit in dealing with issues relating to the collection and management of information by government within a coherent legislative scheme. The Office noted, however, that a fundamental problem with this proposal at the federal level is that the *Privacy Act* extends to both the public and private sectors, while the freedom of information and the archives regimes only extend to the former. The Office suggested that separate privacy legislation could be developed for the private sector, to facilitate a more 'broad brush' approach for government information management, but this would be at the expense of maintaining consistency in relation to privacy regulation.[105]

12.94 The Centre for Law and Genetics submitted that, while there was a very good case for bringing the *Privacy Act* and the FOI Act together, the *Archives Act* has a different and distinct function and should remain separate.[106]

---

101 See, eg, *Freedom of Information and Protection of Privacy Act 1990* RSO c F 31 (Ontario) and *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia).

102 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.19].

103 Ibid, [5.6].

104 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; National Archives of Australia, *Submission PR 199,* 20 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Confidential, *Submission PR 143,* 24 January 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

105 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

106 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

ALRC's view

12.95 The ALRC accepts the concerns expressed in submissions and acknowledges that, despite their many common aspects, each Act has a distinct purpose that is understood by agencies and the public. After considering the views of various stakeholders, the ALRC affirms the view, expressed in ALRC 77, that there is insufficient benefit in the proposal to outweigh the disadvantage in disturbing the current legislative framework. In particular, the fact that the *Privacy Act* regulates both the public and private sectors detracts from the appeal of a single Act.

12.96 One option that may address the interaction of the three Acts is to clarify the objects of each Act. In Chapter 3, the ALRC proposes that the *Privacy Act* be amended to include an objects clause. In ALRC 77, the ALRC and the ARC recommended the amendment of the FOI Act's objects clause and, in ALRC 85, the ALRC proposed an amendment of the *Archives Act* to include an objects clause.[107]

A single regulator?

12.97 One issue for consideration is whether the same body should administer the *Privacy Act* and the FOI Act. This is the case in the Northern Territory,[108] and a number of overseas jurisdictions, for example, the Information and Privacy Commissioner for British Columbia, the Information and Privacy Commissioner Ontario, and the United Kingdom Information Commissioner.[109]

Submissions and consultations

12.98 There was little support for a single body to administer both the *Privacy Act* and the FOI Act. Submissions noted that the *Privacy Act* and the FOI Act have different focuses, and so should be administered by two different bodies.[110] The OPC submitted that

> While there are domestic and international precedents for the creation of one body to perform both functions, the Office is of the view that there may be more than one approach to addressing how these areas should be regulated. In short, these include:
>
> - The *Privacy Act* being the primary mechanism for individuals to access and correct their personal information held in Commonwealth records (regulated by the Privacy Commissioner), while the Commonwealth Ombudsman retains jurisdiction over complaints regarding FOI requests on administrative or policy processes.

---

107 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4 and Rec 1; Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), Ch 4 and Rec 1.

108 See Ch 2.

109 See Office of the Information and Privacy Commissioner for British Columbia, *Website* <www.oipcbc.org> at 30 July 2007; Ontario Information and Privacy Commissioner, *Website* <www.ipc.on.ca> at 30 July 2007; United Kingdom Government Information Commissioner's Office, *Website* <www.ico.gov.uk> at 30 July 2007.

110 Confidential, *Submission PR 143,* 24 January 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007; N Waters, *Consultation PC 17*, Sydney, 2 May 2006.

> • The *Privacy Act* and the FOI Act remain as separate legislation, but are overseen by a single body, such as an Australian Information and Privacy Commissioner.
>
> • The status quo, with separate legislation and separate complaint mechanisms handled by the Privacy Commissioner and the Ombudsman.[111]

12.99 The Office of the Information Commissioner Northern Territory submitted that there are certain advantages in one regulator dealing with both privacy protection and FOI issues.

> It provides a broader perspective when considering issues about disclosure of personal information. Such issues frequently arise under both schemes … I do not believe that oversight of either scheme has been compromised in any way by the combination of the two in the Territory … Having said that, there is certainly an ample scale of work at the Commonwealth level to justify separate offices for oversight of privacy protection and freedom of information.[112]

12.100 A number of stakeholders supported a separate body, such as an Information Commissioner, to oversee freedom of information at the federal level. The Australian Privacy Foundation, for example, submitted that a Freedom of Information Commissioner (FOI Commissioner) is long overdue, as the FOI Act is no longer working as originally intended due to government neglect and outright resistance, and requires an independent champion.[113]

ALRC's views

12.101 The ALRC does not propose the establishment of a single body to administer the *Privacy Act* and the FOI Act. The ALRC notes that the combination of these roles in the Northern Territory and in a number of Canadian provinces appears to work effectively. There was, however, little support for this proposal among stakeholders. Further, the ALRC has made a number of proposals to enhance the role and functions of the Privacy Commissioner. These proposals include enhancing the Commissioner's auditing powers, and new powers in relation to data breach notification and privacy impact assessments. In the ALRC's view, in light of these enhanced powers and the workload that will result, the Privacy Commissioner's focus should continue to be the administration of the *Privacy Act*.

12.102 The Australian Government should, however, establish a body to oversee the administration of the FOI Act. In ALRC 77, the ALRC and the ARC recommended the establishment of a statutory office of FOI Commissioner. The existence of such a statutory office holder would lift the profile of freedom of information, both within

---

111 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

112 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

113 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also, Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

agencies and in the community and would assist applicants to use the FOI Act. It would also give agencies the incentive to accord freedom of information the higher priority required to ensure its effective and efficient administration The ALRC and ARC proposed that the FOI Commissioner's functions should include: auditing agencies' FOI performance, preparing an annual report on FOI, collecting statistics on FOI requests and decisions, publicising the FOI Act in the community, providing FOI training to agencies, and providing information, advice and assistance in respect of FOI requests.[114]

12.103 More recently, a report by the Commonwealth Ombudsman has recommended that the Government consider establishing a FOI Commissioner, possibly as a specialised and separately funded unit in the Office of the Commonwealth Ombudsman.[115] In ALRC 77, the ALRC opposed locating the FOI Commissioner within the Commonwealth Ombudsman's Office. The ALRC's main justification for this was that the Ombudsman's complaint resolution work could reduce the effectiveness of the proposed advice and assistance role of the FOI Commissioner because of a perceived conflict of interests.[116]

12.104 The ALRC notes, however, the broadening role of the Commonwealth Ombudsman since the release of ALRC 77, including its role as the Taxation Ombudsman providing assistance and advice to taxpayers, and its more recent role as Immigration Ombudsman. The Ombudsman also has a number of auditing roles under the *Crimes Act 1914* (Cth), *Telecommunications (Interception and Access) Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth) and the *Anti-Terrorism (No 2) Act 2005* (Cth).[117] More importantly, however, the ALRC notes that the Commonwealth Ombudsman already has a close involvement with freedom of information across all government agencies. In the ALRC's view, it would be appropriate to confer the functions of the FOI Commissioner on the Commonwealth Ombudsman.[118]

Secrecy provisions

12.105 Federal legislation contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office. Secrecy provisions usually are based on the need to preserve the secrecy of government operations in order for government to function effectively.

---

114 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 6 and Rec 18.

115 Commonwealth Ombudsman, *Scrutinising Government: Administration of the Freedom of Information Act 1982 in Australian Government Agencies*, Report No 2 (2006), 33. See also Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.114].

116 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [6.29].

117 Commonwealth Ombudsman, *Scrutinising Government: Administration of the Freedom of Information Act 1982 in Australian Government Agencies*, Report No 2 (2006), [7.12]–[7.14].

118 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), 58.

12.106 The secrecy interests of government agencies and the privacy interests of individuals will sometimes be complementary. For example, both a government agency and the subject of a record that the agency keeps might have an interest in non-disclosure of that information to third parties. Those interests, however, may sometimes conflict. For example, a person may want to access his or her personal information to check that it has been recorded correctly and is not being disclosed without his or her consent; but to grant that access could intrude upon the secrecy interests of the agency.

12.107 There are a number of provisions in federal legislation that create general offences in relation to the unauthorised disclosure of official information.[119] There are also secrecy provisions in federal legislation that deal with unauthorised disclosure of information in specific circumstances.[120] Secrecy provisions in federal legislation are criminal offences that attract criminal penalties. The *Privacy Act*, however, operates as an administrative regime that allows for private remedies such as the award of compensation.[121]

12.108 An example of a secrecy provision is s 5 of the *Australian Prudential Regulation Authority Act 1998* (Cth). This provision states that a person who is or has been an 'officer', including an Australian Prudential Regulation Authority (APRA) member or an APRA staff member, commits an offence if he or she discloses to any person or to a court 'protected information' acquired in the course of his or her duties as an 'officer'. 'Protected information' includes information obtained under a 'prudential regulation framework law' and relating to the affairs of a number of classes of organisations, including a body regulated by APRA. The provision sets out a number of exceptions. For example, it is not an offence if the disclosure of the protected information is for the purposes of a prudential regulation framework law.

12.109 As noted above, the *Privacy Act* includes exceptions to some of the IPPs if acts or practices are required or authorised by or under law. Secrecy provisions that prevent disclosure of information will be consistent with IPP 6 as that principle provides an exception for record-keepers that are required or authorised by a federal

---

119 See, eg, *Crimes Act 1914* (Cth) ss 70 and 79; *Criminal Code* (Cth) s 91.1.

120 See, eg, *Inspector-General of Taxation Act 2002* (Cth) s 37(1); *Gene Technology Act 2000* (Cth) s 187(1); *Aged Care Act 1997* (Cth) s 86-2; *Australian Prudential Regulation Authority Act 1998* (Cth) ss 5, 56; *Australian Postal Corporation Act 1989* (Cth) s 90H; *Civil Aviation Act 1988* (Cth) s 32AP(1); *Australian Institute of Health and Welfare Act 1987* (Cth) s 29(1); *Disability Services Act 1986* (Cth) s 28(2); *Australian Security Intelligence Organisation Act 1979* (Cth) s 92. In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs reported that there were more than 150 secrecy provision in federal legislation and more than 100 different statutes that contain such provisions: Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), xxiv.

121 *Privacy Act 1988* (Cth) pt IIIA creates a range of credit reporting offences: see Ch 55. The ALRC proposes that the *Privacy Act* be amended to provide for civil penalties in limited circumstances: see Proposal 46–2.

law to refuse to provide an individual with access to a record.[122] Further, secrecy provisions that provide for disclosure of protected information in certain circumstances would be consistent with IPP 11, as the disclosure is required or authorised by or under law.[123] The exception under IPP 11(1)(e) in relation to law enforcement, the enforcement of a pecuniary penalty or the protection of the public revenue may also be relevant in some contexts.[124]

12.110 After the release of IP 31, the *Privacy Act* was amended to insert a new Part VIA, which commenced operation on 7 December 2006.[125] The object of the Part is to make special provision for the collection, use and disclosure of personal information in emergencies and disasters. Section 80P(1) provides that at any time when an emergency declaration is in force in relation to an emergency or disaster, an entity may collect, use or disclose personal information in certain circumstances. Section 80P(2) provides that an entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by s 80P(1), unless the secrecy provision is a designated secrecy provision. Designated secrecy provisions include provisions under the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth).[126]

12.111 One issue for consideration is whether there is a need to clarify the relationship between the *Privacy Act* and other legislation containing secrecy provisions. Some secrecy provisions address the operation of the *Privacy Act*. For example, s 5 of the *Australian Prudential Regulation Authority Act* states that a disclosure of personal information under the provision is taken to be authorised by law for the purposes of IPP 11.[127] Other provisions, however, do not address this issue.[128]

12.112 A number of reviews have considered secrecy provisions in federal legislation. The House of Representatives Standing Committee on Legal and Constitutional Affairs considered these provisions in the report *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth*. The Committee found that secrecy provisions had failed to meet adequately the need for flexible regulation of the transfer of information between Commonwealth agencies. The Committee considered that the transfer of personal information between Commonwealth agencies should be regulated

122 Ibid s 14, IPP 6.
123 Ibid s 14, IPP 11.1(d).
124 Taxation legislation includes a number of secrecy provisions which may be said to authorise disclosure of information for the protection of public revenue. See M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt I)' (2002) 8 *Privacy Law & Policy Reporter* 181; M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt II)' (2002) 8 *Privacy Law & Policy Reporter* 193.
125 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).
126 See *Privacy Act 1988* (Cth) s 80P(7).
127 *Australian Prudential Regulation Authority Act 1998* (Cth) s 5(12) also contains a note: 'For additional rules about personal information, see the *Privacy Act 1988* (Cth)'.
128 See, eg, *Disability Services Act 1986* (Cth) s 28.

by the *Privacy Act*, rather than by the secrecy provisions in specific statutes.[129] The Committee also recommended that where federal legislation specifically addresses disclosure or protection of information, the IPPs should not be used to provide additional grounds for disclosure, and that this aspect of the relationship between the IPPs and secrecy provisions should be addressed in the *Privacy Act*.[130]

12.113 The ALRC considered secrecy provisions in its report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98). The ALRC made a number of recommendations, including that the Australian Government should undertake a review of federal secrecy provisions.[131]

12.114 In August 2006, the Treasury released a discussion paper *Review of Taxation Secrecy and Disclosure Provisions*.[132] The Discussion Paper proposed the standardisation and consolidation of the disparate rules under tax legislation that impose strict obligations on tax officers and others who receive tax information.[133] One issue considered by the review was the relationship between the secrecy and disclosure provisions under tax legislation and the *Privacy Act*.[134]

12.115 In January 2007, the Acting Treasurer, the Hon Peter Dutton MP, announced that the secrecy and disclosure provisions from 22 different taxation Acts would, as a result of the review, be standardised into a framework within a single piece of legislation. The standardised secrecy framework would maintain existing authorised disclosures, with the ATO also being able to release taxpayer information in limited circumstances, where the public interest benefits exceed the impact on taxpayer privacy. Newly authorised disclosures would include allowing the ATO to disclose more information to law enforcement agencies.[135]

Submissions and consultations

12.116 In IP 31, the ALRC asked whether the various secrecy provisions under federal legislation that prohibit individuals employed by the Commonwealth from disclosing information contribute to inconsistency and fragmentation in personal information privacy regulation. In particular, the ALRC asked whether the *Privacy Act,*

---

129 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), [4.5], rec 17.

130 Ibid, [4.6] and rec 19. See discussion in Ch 13 relating to 'required or authorised by or under law'.

131 See Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5, Recs 5–1 to 5–5.

132 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006).

133 See, eg, *Income Tax Assessment Act 1936* (Cth) s 16; M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt I)' (2002) 8 *Privacy Law & Policy Reporter* 181; M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt II)' (2002) 8 *Privacy Law & Policy Reporter* 193.

134 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006), App D.

135 The proposed legislation is expected to be introduced into Parliament later this year: P Dutton (Acting Treasurer), 'Providing Increased Certainty on Taxpayer Privacy' (Press Release, 15 January 2007).

rather than secrecy provisions in specific statutes, should regulate the disclosure of personal information by Australian Government agencies.[136]

12.117 A number of government agencies noted that they are subject to secrecy provisions, and that the provisions work well.[137] There was no support for having the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by Australian Government agencies.[138] The Australian Government Department of Employment and Workplace Relations noted that, to avoid confusion, where confidentiality or secrecy provisions are being drafted in new legislation, it may be good practice to deal with the interaction between those provisions and the *Privacy Act* in the legislation or its explanatory material.[139]

12.118 In particular, it was noted that the use of specific statutes allows secrecy provisions to be tailored to particular types of protected information and the situation of the agency.[140] It was also noted in submissions that secrecy provisions can apply to information that includes, but is not limited to, 'personal information', enabling a wider range of information to be protected.[141]

12.119 Protecting all personal information under the *Privacy Act* would not, in some circumstances, provide the level of protection that may be necessary.[142] Some stakeholders noted that providing offences in the *Privacy Act* could be seen as contrary to the 'light-touch' approach that has underpinned the regulation of privacy under the *Privacy Act* to date.[143] The OPC submitted that it was not appropriate for the Privacy Commissioner to administer and enforce secrecy laws.[144]

---

136 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–7.

137 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

138 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

139 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

140 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

141 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

142 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

143 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

144 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

ALRC's view

12.120 The ALRC considers that information that is currently protected by various secrecy provisions in federal legislation should not be regulated by the *Privacy Act*. In the ALRC's view, it is appropriate that specific statutes include secrecy provisions designed to protect information. This ensures that an agency's secrecy responsibilities are tailored to the agency's circumstances and grouped with its other obligations.

12.121 Secrecy provisions do not relate solely to personal information. They also protect other information, for example, commercial information, security details and operational information. Secrecy provisions provide separate and specific standards of protection beyond those afforded by the privacy principles under the *Privacy Act*. Unlike the privacy principles, the level of protection afforded by secrecy provisions will often vary with the sensitivity of the information concerned.

12.122 In the ALRC's view, a privacy impact assessment should be prepared when a secrecy provision in new legislation may have a significant impact on the handling of personal information. In Chapter 44, the ALRC proposes that the *Privacy Act* be amended to empower the Privacy Commissioner to direct an agency or organisation to provide a privacy impact assessment to the Privacy Commissioner in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[145] Further, where a secrecy provision regulates personal information, that provision should address how the requirements under the provision interact with the privacy principles in the *Privacy Act*.

12.123 Secrecy provisions in federal legislation should be reviewed. The need for this review has been established by a number of inquiries. In ALRC 77, the ALRC recommended that 'a thorough review of all federal legislative provisions that prohibit disclosure by public servants of government held information should be conducted as soon as possible to ensure that they do not prevent the disclosure of information that would not be exempt under the FOI Act'.[146] In ALRC 98, the ALRC recommended a review of secrecy provisions to ensure that each provision is consistent with the *Australian Constitution* and to consider the lack of consistency in the fundamental principles and penalty structures in the provisions.[147] The ALRC affirms that the Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.

---

145 See Proposal 44–4.

146 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4, Rec 13. See also Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1320].

147 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5, Rec 5–2.

Obligations of confidence

Common law and equitable duties of confidence

12.124 Legally enforceable obligations to maintain confidence may arise in contract and equity. These obligations are capable of applying to individuals, organisations, agencies and officers of agencies.[148] Relief is available against third party recipients of confidential information, and those who knowingly assist a confidant to breach his or her obligations.[149]

12.125 A contractual obligation of confidence can arise from express terms in a contract, but also by implication.[150] The nature of the obligation will depend on the terms of the contract. Threatened and actual breach of the contractual obligations to maintain confidence attracts the ordinary consequences of threatened and actual breach of contract, including remedies such as injunctions and damages.

12.126 The equitable obligation of confidence can arise where the formalities for contract formation are not present.[151] The obligation arises where information with the necessary quality of confidence about it is imparted in circumstances importing an obligation of confidence.[152] Circumstances importing an obligation of confidence will exist where the information is imparted on the understanding that it is to be treated by the confidant on a limited basis, or where the confidant ought to have realised that in all the circumstances.[153] Breach of the obligation occurs where there is an unauthorised *use*, not only where there is unauthorised *disclosure,* of the information.

12.127 Unlike the position in contract, where loss is the basis of a claim for damages, the plaintiff in a suit for breach of the equitable obligation does not need to show any damage.[154] Remedies for breach of the equitable obligation are equitable compensation or an account of profits, injunction and declaration. There may also be proprietary relief.[155]

---

148 See, eg, *Johns v Australian Securities Commission* (1993) 178 CLR 408, 459–460; *Attorney-General (UK) v Heinemann Publishers Pty Ltd* (1987) 10 NSWLR 86, 191 (McHugh JA).

149 *Johns v Australian Securities Commission* (1993) 178 CLR 408, 459-460; *Breen v Williams* (1996) 186 CLR 71, 129; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [137].

150 *Parry-Jones v Law Society* [1968] 1 All ER 177; R Meagher, *Meagher Gummow & Lehane's Equity: Doctrines & Remedies* (4th ed, 2002), [41–015].

151 Ibid, [41-020].

152 *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 14 FCR 434, 443; *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, 86–87.

153 *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, 86–87; *Coulthard v State of South Australia* (1995) 63 SASR 531, 546–547.

154 *National Roads and Motorists' Association Ltd v Geeson* (2001) 40 ACSR 1, [58]; *NP Generations Pty Ltd v Feneley* (2001) 80 SASR 151, [21].

155 R Meagher, *Meagher Gummow & Lehane's Equity: Doctrines & Remedies* (4th ed, 2002), [41–015].

Statutory protection of confidential information

12.128 Legally enforceable obligations of confidence may also arise under statute. The FOI Act, for example, addresses government confidentiality. Section 45 of the Act protects any document whose disclosure under the Act 'would constitute a breach of confidence'. Federal, state and territory legislation also include a number of confidentiality provisions.[156]

Part VIII of the *Privacy Act*

12.129 In the 1983 report *Privacy* (ALRC 22), the ALRC noted that the English and Scottish Law Commissioner had recommended the establishment of a statutory action for breach of confidence. The ALRC stated that there was little need for a legislative restatement of the circumstances in which a duty of confidence will arise, at least in relation to personal information.[157] The ALRC concluded, however, that the law of duty of confidence, to the extent that it protects privacy interests, should be remedied in three respects:

- where a person is under a duty to preserve confidentiality in respect of personal information, the right to enforce that duty should be extended to the record subject;
- it should be made clear that, as a general rule, personal information to which a duty of confidence applies should remain protected by that duty no matter into whose hands it might subsequently come; and
- the remedies available under common law and equity should be rationalised so that in each case both injunctions and damages on the same bases will be available to the person seeking to enforce the duty.[158]

12.130 The introduction of Part VIII of the *Privacy Act* implemented the ALRC's recommendations in relation to obligations of confidence 'to which an agency or a Commonwealth officer is subject, however the obligation arose' or 'that arises under or by virtue of the law in force in the Australian Capital Territory'.[159]

12.131 Part VIII of the *Privacy Act* applies only to situations where a person (a 'confidant') is subject to an obligation of confidence to another person (a 'confider') in respect of personal information. The obligation applies whether or not the information relates to the confider or to a third person.[160] It generally preserves all other laws, principles or rules 'under or by virtue of which an obligation of confidence exists',

---

156 See discussion of *Privacy Act 1988* (Cth) pt 8 below and discussion of other confidentiality provisions in Chs 13, 56.

157 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1312].

158 Ibid, [1312]–[1314].

159 *Privacy Act 1988* (Cth) s 89; Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General).

160 *Privacy Act 1988* (Cth) s 90.

except as expressly qualified, or by necessary implication. It also preserves laws, principles or rules that 'have the effect of prohibiting, or imposing a liability (including a criminal liability) on a person in respect of, a disclosure or use of information'.[161] Part VIII, therefore, allows for the fact that obligations of confidence may arise in various ways.

12.132 The operative provisions are ss 92 and 93. Section 92 essentially extends the obligation a confidant owes to a confider to a third party who acquires the information knowing, or being in a position where he or she ought reasonably to know, that the person from whom he or she acquired the information was subject to an obligation of confidence. Section 93 concerns relief for breach of the obligation. Without limiting any other right a confider has to relief in respect of a breach,[162] a confider under s 93(1) 'may recover damages from a confidant in respect of a breach of an obligation of confidence with respect to personal information'.[163]

12.133 Where the information the subject of the confidence is personal information relating to a third person, that person 'has the same rights against the confidant in respect of a breach or threatened breach of the obligation as the confider has'.[164] This is an important extension on the general law position.

12.134 Courts of the ACT are conferred jurisdiction regarding 'matters' arising under Part VIII, which is also said not to deprive 'a court of a State or of another Territory of any jurisdiction that it has'.[165] There are no known court decisions (reported or unreported) applying the confidentiality provisions.

Submissions and consultations

12.135 In IP 31, the ALRC asked whether the provisions in Part VIII of the *Privacy Act* are necessary, and whether the provisions are adequate and should be contained in the *Privacy Act* or elsewhere.[166]

12.136 The OPC submitted that it does not have any experience in the application of Part VIII because the provisions do not confer any powers on the Office to determine matters or provide a remedy.[167] The Australian Privacy Foundation submitted that neither the objectives of Part VIII, nor the circumstances in which they might apply, are clear.[168] The Centre for Law and Genetics submitted that if the provisions of the

---

161 Ibid s 91.
162 Ibid s 93(2).
163 Since s 93(1) does not limit or restrict any other right that the confider has in respect of the breach, he or she will continue to have a claim to the remedy of equitable compensation where the obligation arises in the equity jurisdiction rather than, for example, in contract. The assessment of 'damages' under s 93(1) will not necessarily use the same criteria of quantum, causation, remoteness etc as those that apply to assessment of equitable compensation, or to assessment of damages in contract or for any other civil wrong.
164 *Privacy Act 1988* (Cth) s 93(3).
165 *Privacy Act 1988* (Cth) s 94.
166 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006) Question 7–8.
167 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
168 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

Part do not appear to have been widely used they should be deleted.[169] Ian Turnbull submitted, however, that Part VIII is necessary and might be extended to cover private sector confidences such as health professionals.[170]

ALRC's view

12.137 The ALRC considers that the confidentiality provisions contained in Part VIII of the *Privacy Act* should be repealed. The ALRC notes that the provisions have never been used. It is hard to imagine when this action would be used in preference to making a complaint to the OPC about a breach of the IPPs (or the proposed UPPs) under the *Privacy Act*.

12.138 Part VIII represents an extension of the law of confidentiality in that it extends the right to enforce a duty of confidentiality to the record subject. This right is not provided for under Australian common law.[171]

12.139 As discussed in Chapter 5, the English courts have developed the action for breach of confidence so that it now covers the disclosure of information that the defendant knows, or ought to know, is private because such disclosure is a wrongful invasion of privacy.[172] The ALRC shares the view of the New South Wales Law Reform Commission (NSWLRC) that the common law of Australia is unlikely to, and should not, follow the English example of transforming breach of confidence in this way. The NSWLRC has listed three reasons why this is so:

> First, confidentiality and privacy are simply different concepts … While most confidential acts and information could arguably be described as private, not all private activity is necessarily confidential.
>
> Secondly, the doctrine of breach of confidence, developed primarily in the exclusive jurisdiction of equity, seems an unsuitable vehicle for the introduction and development of greater privacy protection … equitable intervention does not fasten on the intrinsic value of the information itself.
>
> Thirdly, although the legal notion of confidence is not necessarily restricted to the disclosure of 'information' in any technical sense, it is unclear to what extent breach of confidence would be useful beyond situations involving the unjustified publication of private information.[173]

12.140 The ALRC considers that rather than extending the law of confidentiality, it is more appropriate to enact a statutory cause of action for invasion of privacy. The cause of action will apply to both agencies and organisations, unlike Part VIII which only applies to agencies; will provide broader protection of privacy than that offered by

---

169 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
170 I Turnbull, *Submission PR 82,* 12 January 2007.
171 *Commonwealth v John Fairfax & Sons Ltd* (1980) 147 CLR 39, 51.
172. See *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920; *Ash v McKennitt* [2007] 3 WLR 194.
173 New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007).

Part VIII; and will offer a range of remedies. The ALRC's proposal for a statutory cause of action is outlined in Chapter 5.

Proposal 12–14 Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

13. Required or Authorised by or Under Law

Contents

Introduction 487
'Required or authorised by or under law' 487
Scope of the exception 488
Relationship between the *Privacy Act* and other federal laws 491
'Specifically authorised' 491
Submissions and consultations 492
ALRC's view 494
Census and Statistics Act 1905 (Cth) 498
Submissions and consultations 500
ALRC's view 501
Corporations Act 2001 (Cth) 502
Submissions and consultations 504
ALRC's view 506
Commonwealth Electoral Act 1918 (Cth) 506
Submissions and consultations 507
ALRC's view 509
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) 510
Background 511
Submissions and consultations 513
ALRC's view 516

Introduction

13.1 An act or practice 'required or authorised by or under law' is an exception to a number of the limits on the handling of personal information under the *Privacy Act*. This chapter first considers what is meant by the phrase 'required or authorised by or under law', and outlines a new exception for acts and practices that are 'specifically authorised by or under law'. The chapter then considers a number of federal Acts that require or authorise acts and practices for the purposes of the *Privacy Act*. These laws include the *Census and Statistics Act 1905* (Cth), *Corporations Act 2001* (Cth), *Commonwealth Electoral Act 1918* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act). The interaction between these laws and the *Privacy Act* has been the subject of recent public debate.

'Required or authorised by or under law'

13.2 An act or practice required or authorised by or under law is an exception (the 'required or authorised exception') to a number of the Information Privacy Principles

(IPPs) and the National Privacy Principles (NPPs).[1] For example, IPP 11(1)(d) provides that a record-keeper may disclose personal information to a person, body or agency if the disclosure is required or authorised by or under law. NPP 2.1(g) similarly provides that an organisation may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under law. The required or authorised exception also applies to other areas of the *Privacy Act*.[2]

13.3 The ALRC proposes that acts or practices that are required or authorised by or under law should be an exception to a number of the proposed Unified Privacy Principles (UPPs), including the 'Collection' principle, 'Specific Notification' principle, 'Use and Disclosure' principle, and 'Access and Correction' principle.

13.4 State and territory privacy laws include similar exceptions. For example, s 25 of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that it is an exception to various Information Privacy Principles under that Act if an agency is 'lawfully authorised or required not to comply with the principle concerned', or 'non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law'.[3]

Scope of the exception

'Required' by or under law

13.5 The Office of the Privacy Commissioner (OPC) states that the 'required' by or under law exception in the context of IPP 2 'is only appropriate in the rare case where the agency has no choice in whether or not it collects the information'.[4] This interpretation is consistent with interpretations of 'required' in the context of other laws.[5]

13.6 The Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) states that the exception is intended to cover situations where a law unambiguously requires a certain act or practice. It also suggests, however, that a law could require an act or practice by implication.

---

1 *Privacy Act 1988* (Cth) s 14, IPPs 5.2, 6, 10.1(c), 11.1(d); sch 3, NPPs 2.1(g), 6.1(h).

2 See, eg, Ibid ss 6D(7)(c), 18L.

3 See also Principle 9 in the *Health Records (Privacy and Access) Act 1997* (ACT) which provides an exception to the use of personal health information if the use is required or authorised by a law of the ACT, a law of the Commonwealth, or an order of a court of competent jurisdiction. Principle 2 (Use and Disclosure) of the *Health Records Act 2001* (Vic) provides an exception for uses and disclosures that are 'required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law)'.

4 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 21. See also *Re VBN and Australian Prudential Regulation Authority* (2006) 92 ALD 475.

5 See, eg, *Chamberlain v Banks* (1985) 7 FCR 598 (*Administrative Decisions (Judicial Review) Act 1977* (Cth) s 5(1)(b)); *Department of Premier & Cabinet v Hulls* [1999] 3 VR 331 (*Freedom of Information Act 1982* (Vic) s 50(4)).

> There could be situations where the law requires some actions which, of necessity, involve particular uses or disclosures, but this sort of implied requirement would be conservatively interpreted.[6]

13.7 The OPC also suggests this interpretation of the exception in the context of IPP 10 (Limits on use of personal information). The OPC states that an agency may be required by law to use personal information for another purpose if the agency is governed by legislation that requires it to perform a specific function, and the only possible way the agency can perform that function is by using the particular information for a purpose different from that for which it was obtained.[7]

'Authorised' by or under law

13.8 While an agency or an organisation that is 'required' by law to engage in an act or practice has no choice in the matter, an agency that is 'authorised' by law has a discretion as to whether it will engage in an act or practice.[8]

13.9 In the opinion of the OPC, an act or practice is not 'authorised' solely because there is no law prohibiting it.[9] Further, the law that authorises an act or practice must provide a 'specific relevant discretion'. For example, a general provision that a statutory office holder or the head of an agency may do anything necessary or convenient to be done for or in connection with a function does not meet this criterion.[10]

13.10 A law can also impliedly 'authorise' an act or practice. The OPC has stated in the context of the required or authorised exception to IPP 10 and IPP 11:

> A use or disclosure may fall within 10.1(c) or 11.1(d) if the law requires or authorises a function or activity that clearly and directly entails the use or disclosure. Here, the use or disclosure is impliedly authorised by law because it is essential to effect a scheme the law lays down.[11]

'Law'

13.11 What kinds of laws can require or authorise acts or practices for the purposes of the exception? Only a few cases have considered what is meant by 'law' for the

---

6 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 139.
7 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996).
8 Ibid.
9 Ibid.
10 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998).
11 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996).

purposes of the required or authorised exception. It has been held that 'law' in the context of the exception includes a federal Act[12] and court rules.[13]

13.12 The OPC's *Guidelines to the National Privacy Principles* provide that 'law' includes Commonwealth, state and territory legislation, as well as common law.[14] The OPC *Plain English Guidelines to the Information Privacy Principles* provide more detailed advice on the meaning of 'law'. The Guidelines provide that 'law' for the purposes of the required or authorised exception to IPP 10 and IPP 11 means Commonwealth acts and delegated legislation, and state and territory laws where the state has 'validly legislated to bind the Commonwealth'. The OPC also states that 'law' includes:

- documents with the force of Commonwealth law (a document may have the 'force of law' if it is an offence to breach its provisions, or it is possible for a penalty lawfully to be imposed if its provisions are breached, for example, industrial awards);
- disclosures to Commonwealth ministers; and
- Commonwealth parliamentary privilege.[15]

13.13 The OPC states that a number of laws are normally not accepted as 'law' for the purpose of the required or authorised exception, including:

- state law that does not validly bind the Commonwealth;
- Cabinet decisions;
- inter-agency agreements and contracts between an agency and other parties;
- common law; and
- requests for personal information from foreign governments.[16]

13.14 Common law, for these purposes, 'consists of broad statements of legal principle and is made by judges—as opposed to statute law which is legislation made by Parliament'. The Privacy Commissioner has occasionally accepted that a disclosure

---

12 *Re VBN and Australian Prudential Regulation Authority* (2006) 92 ALD 475.

13 *Re An Application by the NSW Bar Association* [2004] FMCA 52.

14 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.

15 The OPC notes, however, that if the *Privacy Act* would prohibit the disclosure were it not for parliamentary privilege, it may be appropriate for the agency to approach its Minister with any concerns it has about disclosing the personal information: Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996).

16 These requests will only fall within exceptions 10.1(c) or 11.1(d) of the *Privacy Act* if there is a Commonwealth law that requires or authorises the agency to provide personal information in those circumstances. Similarly, treaty obligations only fall within these exceptions if there is a Commonwealth law that enacts that obligation: Ibid.

is necessary to satisfy requirements imposed by the common law principle of natural justice.[17]

13.15 State and territory courts and tribunals have held that the meaning of 'law' in relation to similar exceptions under state and territory privacy laws includes a common law duty of care to warn;[18] a subpoena to disclose information to a court;[19] and a warrant to obtain records from a hospital under a state Act.[20] In its submission to the NSW Attorney General's Department review of the *Privacy and Personal Information Act 1998* (NSW), Privacy NSW stated that the scope of 'other law' in s 25 of the Act is unclear.[21]

Relationship between the *Privacy Act* and other federal laws

13.16 Federal legislation contains a number of provisions that authorise or require certain acts or practices for the purpose of the *Privacy Act*. Most of these provisions are related to the disclosure of personal information.[22] For example, s 42(1)(g) of the *Australian Passports Act 2005* (Cth) provides that the Minister performing functions under the Act may request certain persons to disclose personal information about a person to whom an Australian travel document has been issued. Section 42(3) then provides that, for the purposes of IPP 11(1)(d) and NPP 2.1(g), such a disclosure is required or authorised by law.

13.17 The interaction between these provisions and the *Privacy Act* is, however, not always clear. For example, some provisions under federal legislation authorise or require disclosure of information, but do not state that it is required or authorised for the purposes of the *Privacy Act*.[23] Other provisions, such as s 488B of the *Migration Act 1958* (Cth), provide that certain disclosures of information may occur 'even if the information is personal information (as defined in the *Privacy Act 1988*)'.[24]

'Specifically authorised'

13.18 While acts and practices that are 'required' by law will be relatively rare, the 'authorised' by or under law exception could except a wide range of acts and practices from the limits imposed by the *Privacy Act*. One issue for consideration is whether the 'authorised' by or under law exception should be narrowed. One option would be to

---

17 Ibid.

18 *Director General Department of Education and Training v MT* [2005] NSWADTAP 77.

19 *HW v Commissioner of Police* [2003] NSWADT 214.

20 *Royal Women's Hospital v Medical Practitioners Board of Victoria* (2006) 15 VR 22.

21 Privacy NSW, *Submission to the New South Wales Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2004, 88.

22 See, eg, *Australian Passports Act 2005* (Cth) s 42; *Building and Construction Industry Improvement Act 2005* (Cth) s 65; *Military Rehabilitation and Compensation Act 2004* (Cth) s 409; *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 3A; *Telecommunications Act 1997* (Cth) s 303B; *Wheat Marketing Act 1989* (Cth) s 59; *Veterans' Entitlements Act 1986* (Cth) s 38AA; *Migration Act 1958* (Cth) ss 321 and 336FB.

23 See, eg, *Snowy Hydro Corporatisation Act 1997* (Cth) s 56; *Wheat Marketing Act 1989* (Cth) s 59.

24 See also *Customs Act 1901* (Cth) ss 64ACA, 64ACB, 64AF and 273GAB.

provide a new exception to certain principles if an act or practice is 'specifically authorised'. The European Union Article 29 Data Protection Working Party has criticised the required or authorised exception under the *Privacy Act* as being imprecise:

> The wording 'authorised' as opposed to 'specifically authorised' which existed in the January 1999 edition of the National Principles can also be read to mean that all secondary purposes that are not forbidden are allowed. In the working party's view such a wide exemption would virtually devoid the purpose limitation principle of any value.[25]

13.19 The term 'specifically authorised' is used in a number of federal Acts. Section 51 of the *Trade Practices Act 1974* (Cth) provides that, in deciding whether a person has contravened Part IV of the Act (restrictive trade practices), anything specified in, or 'specifically authorised' by certain laws must be disregarded. Section 43A of the *Environment Protection and Biodiversity Conservation Act 1999* (Cth) refers to 'specific environmental authorisation'. The Federal Court of Australia considered the meaning of this phrase in *Minister for the Environment & Heritage v Greentree (No 2)*. In that case, Sackville J considered whether the respondents were specifically authorised to undertake certain activities on land that was 'declared Ramsar wetland'.

> The language of s 43A(1)(b) of the EPBC Act implies that there is a distinction between an action which is authorised under an Act and one which is specifically authorised … in my view [specifically authorised] does not mean that the authorisation must only relate to a single site or to a single activity on land. It is in my view enough that the authorisation covers a defined class of activities or identifiable land which includes the subject land.[26]

13.20 As noted above, a reference to 'authorised' has been interpreted as including law that impliedly authorises an act or practice in certain circumstances. A law that 'specifically authorised' an act or practice would only include a law that expressly authorises an act or practice. 'Specifically authorised' could also be confined to authorisations that relate to a defined class of acts and practices.

Submissions and consultations

13.21 In Issues Paper 31, *Review of Privacy* (IP 31), the ALRC asked whether any difficulties arise as a result of the interaction between the *Privacy Act* and provisions in other federal legislation that require or authorise acts or practices that would otherwise be regulated by the IPPs or the NPPs. The ALRC was also interested in how the interaction between the *Privacy Act* and these provisions should be clarified.[27]

13.22 The Australian Privacy Foundation suggested an alternative formulation of the required or authorised exception:

---

25 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 4.

26 *Minister for the Environment & Heritage v Greentree (No 2)* [2004] FCA 741, [153].

27 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–5.

> We submit that a basic distinction should be made between other laws which expressly require particular uses and disclosures should form exceptions to the use and disclosure principles in the *Privacy Act*, but that where acts or practices are only 'authorised' then the use and disclosure principles in the *Privacy Act* should prevent use and disclosure unless another exception applies ie mere lawful authority (which is understood to include common law and contractual authorities) should not in itself be grounds for use and disclosure for secondary purposes without consent.[28]

13.23 Stakeholders submitted that legislation which intends to rely on the required or authorised exception should include clear references in the legislation.[29] The OPC submitted that

> legislation should expressly set out its intention to require or authorise a particular use or disclosure (such as by directly referring to the *Privacy Act*). This helps to avoid interpretations or implications that allow the personal information to be handled in ways that legislators did not intend.[30]

13.24 It was noted that ambiguity in legislation can cause uncertainty for agencies and individuals and, potentially, the OPC as to how information should be handled, and whether the relevant provision meets the requirements under the *Privacy Act*.[31]

13.25 The Office of the Information Commissioner Northern Territory and the Office of the Victorian Privacy Commissioner (OVPC) noted that legislation that predates the *Privacy Act* may continue to provide justification for what would otherwise constitute breaches of privacy principles. Both these submissions emphasised the importance of requiring any legislation that raises privacy issues to be reviewed at appropriate intervals to confirm that the Parliament continues to accept that it reflects an appropriate balance between privacy interests and other interests.[32]

13.26 One stakeholder submitted that the *Privacy Act* needs to be redrafted to clarify the meaning of particular terms referred to in the IPPs. This submission also questioned the OPC's interpretation that the required or authorised exception does not include acts or practices that are required or authorised by the common law.[33]

13.27 Noting the OPC's statement in the *Plain English Guidelines to the Information Privacy Principles* that the common law consists of 'broad statements of legal principle', it was submitted that the common law may prescribe an act or practice with considerable particularity.[34] It was also submitted that there is a strong case from the

---

28 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
30 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
31 Ibid.
32 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. See also Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.
33 Confidential, *Submission PR 165,* 1 February 2007.
34 Ibid.

perspective of federal and international comity for giving the term 'law' its widest possible meaning. It is not clear, for example, why the OPC would consider that a state law imposing a pecuniary penalty is any the less a 'law' for the purposes of the use and disclosure principles.[35]

13.28 The OPC suggested that a consolidated digest could be developed, listing all legislative provisions that require or authorise personal information to be handled in ways that the *Privacy Act* may otherwise prevent. It was submitted that this could clarify the scope of particular legal provisions and their relationship to the *Privacy Act*, keep track of the number and extent of lawful exceptions to the *Privacy Act*, and improve public confidence in legal transparency.[36] The OPC suggested that such a project may require the coordination of numerous agencies and organisations, such as the OPC and, possibly, the Australian Government Attorney-General's Department.[37]

ALRC's view

Scope of the required or authorised exception

13.29 In the ALRC's view, the *Privacy Act* should not fetter a government's discretion to require or authorise that personal information be handled in a particular way. There is a public expectation that governments are able to make laws to facilitate the handling of information in certain appropriate and necessary ways. The required or authorised exception reflects this expectation.[38] The scope of the exception does, however, require clarification. Submissions noted that the ambiguity in the operation of this exception can create uncertainty for individuals, agencies, organisations and privacy regulators.

13.30 While the scope of 'required' and 'authorised' appear to be well understood, the categories of laws that are 'law' for the purposes of the exception is less clear. In the ALRC's view, federal acts and delegated legislation are clearly 'law' for the purpose of the exception. These laws are subject to various accountability requirements including the scrutiny of Parliament and disallowance. These accountability requirements help to ensure that any reliance on the required or authorised exception is appropriate and justified.

13.31 'Law' should also include state and territory Acts and delegated legislation. These laws are also subject to accountability requirements. If state and territory laws were not considered law for the purposes of the exception, an organisation, for example, could find that they were subject to conflicting obligations under the *Privacy Act* and a state or territory Act or delegated legislation.

13.32 It is not clear to what extent a 'law' for the purposes of the required or authorised exception includes a common law or equitable duty. The ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical

35 Ibid.
36 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
37 Ibid.
38 Ibid.

Research Council considered this issue in *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96). The ALRC and AHEC noted that:

> It appears to be accepted that 'law' may include the common law. However, it is not entirely clear whether NPP 2.1(d) permits a doctor to disclose confidential information where the disclosure is covered by the public interest exception to the common law duty of confidentiality. In an Attorney-General's Department information paper, the Government acknowledged that the health profession had a strong respect for the confidentiality of health information and maintained sound privacy practices. The paper stated that the 'legislation is not intended to interfere with those professional values and standards'.[39]

13.33 The ALRC and AHEC concluded that the application of the *Privacy Act* to the disclosure of health information by doctors and other health professionals, in circumstances that may not breach common law or ethical requirements of confidentiality, may require clarification.[40]

13.34 Further, it is unclear whether 'law' should include an order of a court or tribunal; documents that are given the force of law by an Act of Parliament, such as industrial awards; or statutory instruments such as Local Environmental Plans made under planning laws. The ALRC is interested in hearing stakeholder views on whether these laws should be regarded as a 'law' for the purposes of the required or authorised exception.

Question 13–1 Should the definition of a 'law' for the purposes of determining when an act or practice is required or specifically authorised by or under a law include:

(a) a common law or equitable duty;

(b) an order of a court or tribunal;

(c) documents that are given the force of law by an Act of Parliament, such as industrial awards; and

(d) statutory instruments such as a Local Environmental Plan made under a planning law?

Review of legislation

13.35 Submissions emphasised that legislation that raises privacy issues should be reviewed at appropriate intervals to confirm that Parliament continues to accept that it reflects an appropriate balance between privacy interests and other interests.

---

39 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [21.56].

40 Ibid, [21.56].

13.36 The ALRC notes that the Privacy Commissioner currently has various powers that would allow her to review legislation for these purposes. These powers include a power under s 27(1)(f) to provide, on request or on the Commissioner's own initiative, advice to a minister, agency or organisation on any matter relevant to the operation of the *Privacy Act*. In the ALRC's view, this power enables the Privacy Commissioner to monitor legislation that requires or authorises certain acts and practices for the purposes of the *Privacy Act*, and provide advice to the minister responsible for that legislation, if those acts and practices are no longer considered appropriate.

Clear references to exception in legislation

13.37 Another option is to amend legislation which is intended to rely on the required or authorised exception so that it includes clear reference to this in the legislation.[41]

13.38 In the ALRC's view, legislation should clearly set out whether it is intended to require or authorise an act or practice for the purposes of the *Privacy Act.* In the interest of clarity and transparency, these provisions should set out the type of information to be dealt with, the scope of the requirement or authorisation, and the extent to which the *Privacy Act* applies to the handling of that information.

13.39 It would be too onerous to amend all federal, state and territory legislation that may require or authorise an act or practice in relation to the handling of personal information. Federal, state and territory parliaments should, however, ensure that proposed laws that are intended to rely on the required or authorised exception include clear references to the exception. This task could be undertaken as part of a privacy impact assessment.[42]

A list of laws that require or authorise acts and practices

13.40 One option raised by the OPC is the compilation of a list of provisions in other legislation that require or authorise acts or practices that would otherwise be regulated by the *Privacy Act*. Such a list of laws would provide clarity for agencies, organisations, individuals and privacy regulators about whether certain laws met the criteria of the exception.

13.41 The list could act as a centralised resource for drafting and, potentially, the development of a standardised provision. The list could also serve an educative function in that it may prompt agencies to consider privacy implications when developing legislation.

13.42 This proposal raises a range of issues. A threshold question is whether the list should have the force of law. One option is to locate the list in a schedule to the *Privacy Act*. Including the list as a schedule to the Act would make it easy for people to find and would give the list authority. Updating the list, however, would require legislative amendment and be time consuming, affecting the currency of the list.

---

41 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

42 See Chs 4, 11 and 44.

Promulgating the list in regulations may be a more appropriate option. Regulations are used to give force of law to matters that are subject to frequent change.

13.43 A less formal method is for the list to published on the website of the Attorney-General's Department or the OPC. While this option provides for flexibility and accessibility, the list will not have the same legal authority as a schedule to the *Privacy Act*.

13.44 A further issue is whether the list should be comprehensive or indicative. The list could be restricted to the required or authorised exception to the proposed UPPs or cover the operation of the exception in the context of other provisions of the *Privacy Act*. Another question is whether the list should contain federal laws only, or whether it should also include state and territory laws, and common law duties. The list could be restricted to future provisions or extend to existing provisions. One concern is that the practice of identifying some provisions and not others could produce an interpretation that listing was a necessary precondition for the exception to operate.

13.45 Another issue for consideration is who should be responsible for the preparation of such a list. One option would be for the OPC to compile the list. It is, however, questionable whether the OPC would have the resources to undertake such a task. Another option would be to have the Australian Government Attorney-General's Department compile the list. Agency heads could supply to the Department a list of provisions in legislation they administer that require or authorise the handling of personal information. The ALRC is interested in comment on these issues.

Question 13–2 Should a list be compiled of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*? If so, should the list have the force of law? Should it be comprehensive or indicative? What body should be responsible for compiling and updating the list?

Specifically authorised

13.46 In the ALRC's view, the required or authorised exception is essential to grant governments the discretion to provide that personal information be handled in particular ways. The ALRC has, therefore, proposed that it remain as an exception to a number of the proposed UPPs.

13.47 The ALRC has, however, identified two areas where an exception in relation to acts and practices that are 'specifically authorised' by or under law would be beneficial. An exception for acts and practices that are 'specifically authorised' would require the law expressly to authorise a defined class of acts and practices. In the ALRC's view this exception would require the Australian Parliament and state and territory parliaments to have turned their mind to how the proposed law interacts with

the *Privacy Act*, and to the competing interests for and against the handling of personal information in a particular context.

13.48 The ALRC proposes the use of the specifically authorised exception in the context of the proposed 'Collection' and 'Specific notification' principles. NPP 10.1(b) currently provides that an organisation must not collect sensitive information about an individual unless the collection is required by law. In the ALRC's view, this exception is too narrow. The ALRC considered proposing an exception to the 'Collection' principle if an act or practice was 'authorised by law'. Such an exception would be too wide as it could include laws that impliedly authorise certain acts and practices. Therefore, in Chapter 19, the ALRC proposes that an agency or an organisation must not collect sensitive information unless the collection is required or specifically authorised by or under law.[43]

13.49 The ALRC also proposes a new 'Specific Notification' principle that requires agencies and organisations to take reasonable steps to inform an individual of certain matters, except to the extent that the agency is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.[44] In the ALRC's view this solution strikes an appropriate balance between making agencies and organisations generally accountable for the personal information they collect and recognising that, in certain situations and where it is provided for expressly in a law, the requirements of accountability and transparency should be relaxed in favour of other considerations.

Census and Statistics Act 1905 (Cth)

13.50 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).[45] The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, industry, businesses and private individuals.

13.51 In the late 1970s, the ALRC conducted an inquiry into privacy issues and the census, culminating in the release in 1979 of the report *Privacy and the Census* (ALRC 12).[46] The report made a number of recommendations directed to the protection of personal information collected as part of the census.[47] A number of these recommendations have been implemented.[48]

---

43 See Ch 19 and proposed 'Collection' principle.
44 See Ch 20 and proposed 'Specific Notification' principle.
45 *Census and Statistics Act 1905* (Cth) s 8.
46 Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).
47 Ibid, x–xvi.
48 See, eg, *Census Information Legislation Amendment Act 2000* (Cth).

13.52 The *Privacy Act* was enacted in 1988. The *Privacy Act* applies the IPPs to personal information collected as part of the census.[49] Under the *Privacy Act*, personal information collected by the ABS for a census is collected for a lawful purpose directly related to a function or activity of the ABS and is necessary and directly related to that purpose.[50] The *Census and Statistics Act* also contains a number of provisions, including secrecy provisions, directed to the protection of information collected as part of the census.[51] For example, s 19A provides that the Australian Statistician or an ABS officer must not at any time, during the period of 99 years from the day for a census, divulge or be required to divulge information contained in a census form to an agency, a court or a tribunal.[52]

13.53 Before the 2001 Census, all name-identified information from past census was destroyed on completion of statistical processing. In 2000, the Australian Government introduced legislation that provided for the retention of census data.[53] This legislation was put in place for the 2001 Census on a trial basis. The *Census Information Legislation Amendment Act 2006* (Cth) amended the *Census and Statistics Act* to ensure that, subject to the household's consent, name-identified information collected in the 2006 Census and all subsequent census would be stored by the National Archives of Australia to be preserved for release for future research after a closed access period of 99 years.[54]

13.54 Another recent development is the Census Data Enhancement (CDE) project.[55] The primary objective of the CDE project was to enhance the value of the census by combining it with future census and, possibly, other datasets held by the ABS. The central feature would have been the Statistical Longitudinal Census Dataset (SLCD) involving all respondents to the census. A Discussion Paper on the project was released in April 2005[56] and a privacy impact assessment (PIA) was prepared.[57] Although there

---

49 The ABS is an 'agency' for the purposes of the *Privacy Act*: *Privacy Act 1988* (Cth) s 6. For a discussion of how the IPPs apply to the census see Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Saving Our Census and Preserving Our History* (1998), Ch 4.

50 *Privacy Act 1988* (Cth) s 14, IPP 1.1.

51 *Census and Statistics Act 1905* (Cth) ss 7, 8A, 13, 19, 19A, and 19B. Further, the *Statistics Determination 1983* (Cth) made by the Minister under *Census and Statistics Act 1905* (Cth) s 13 provides for the disclosure, with the approval in writing of the Statistician, of specified classes of information.

52 See Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Saving Our Census and Preserving Our History* (1998), rec 1. See also Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

53 *Census Information Legislation Amendment Act 2000* (Cth).

54 Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth). In 2001, 52% of Australians gave consent to have their name-identified information released after 99 years. For 2006, the participation rate was 56.1%: Australian Bureau of Statistics, 'Retention Facts and Figures (the Census Time Capsule)' (Press Release, 27 June 2007).

55 Australian Bureau of Statistics, *Census of Population and Housing—Census Data Enhancement* <www.abs.gov.au> at 31 July 2007.

56 Australian Bureau of Statistics, *Enhancing the Population Census: Developing a Longitudinal View* (2005).

57 Pacific Privacy Consulting, *Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics* (2005).

was some support for the project, a number of submissions and the PIA identified significant privacy-related concerns.[58] In particular, the PIA noted that the proposal

> will create a data resource so rich and valuable for administrative uses that the privacy and secrecy framework under which the ABS operates may come under great and possibly irresistible pressure, if not immediately, then at least in the medium to long term …
>
> Despite the rigour of the legislative protections, and the ABS track record both of procedural safeguards and of defence of the principle of confidentiality, there remains a residual privacy risk of future changes in legislation to allow administrative and other nonstatistical uses.[59]

13.55 On 18 August 2005, the ABS announced that it would not proceed with the SLCD as proposed and that the CDE proposal had been substantially modified.[60] The SLCD will now be based on a 5% sample of the population. In the ABS's view, the reduction of the dataset to a 5% sample will make the dataset unsuitable for administrative and other non-statistical uses.

Submissions and consultations

13.56 In IP 31, the ALRC asked whether personal information collected pursuant to the *Census and Statistics Act* was adequately protected.[61] The ABS submitted that the *Census and Statistics Act* adequately protects personal information collected under it.

> When the ABS publishes statistics, or releases information, it cannot do so in a manner that is likely to enable the identification of a particular person. In order to ensure the ABS complies with this requirement, the ABS has developed statistical methods to prevent the disclosure of identifiable information, while allowing sufficiently detailed information to be released to make the statistics useful.[62]

13.57 The OPC agreed that the legislative protections afforded by the *Privacy Act* and the secrecy provisions of the *Census and Statistics Act* provide a sound framework for the appropriate handling of personal information. The OPC noted, however, that it is aware of concerns held by some individuals in the community regarding the census, including about: the amount of detail collected for household surveys and whether some of the questions are unnecessarily intrusive; the powers of the ABS to compel individuals to disclose personal information; whether collectors can see the information; whether the personal information is handled securely while in transit; and

---

58 See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.113]–[5.116].

59 Pacific Privacy Consulting, *Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics* (2005), 3.

60 Australian Bureau of Statistics, 'ABS Develops a New View of Records Across Successive Censuses' (Press Release, 18 August 2005).

61 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(i).

62 Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

the degree to which personal information may be available to others. These concerns are generally most pronounced in the period leading up to the taking of the census.[63]

13.58 The Australian Privacy Foundation submitted that any further erosion of the confidentiality provisions of the *Census and Statistics Act* needs to be resisted firmly, not only because of the extraordinary sensitivity of much census information, but also because of the public interest in truthful and therefore reliable census responses.

> We consistently drew attention during the 1990s to the Bureau of Statistics as the one and only Commonwealth agency which could give unqualified assurances of confidentiality. Regrettably this is no longer the case since the introduction in 2005 of the Longitudinal Data Set (albeit on a sample basis), and in the last two censuses of the 'opt in' retention of forms by the Australian Archives, for access by researchers after 99 years.[64]

ALRC's view

13.59 The ALRC does not make a proposal in relation to the operation and administration of the *Census and Statistics Act*. The information contained in name-identified census records and released after 99 years is an invaluable source for historians, historical sociologists and other researchers; and is adequately protected under the current regime.

13.60 The ALRC notes that the collection and retention of name-identified information is only to occur with the consent of the individual.[65] This is consistent with the current IPPs and the proposed UPPs. Further, in the ALRC's view the sensitivity of much personal information has diminished after 99 years. The legislated closed period of 99 years is a recognition of this fact.

13.61 The retention of records by the National Archives of Australia for a period of 99 years is consistent with IPP 4 (Storage and security of personal information). The protection provided by the *Archives Act 1983* (Cth) is robust and beyond that accorded to other personal information.[66] During the time it is in the closed period, the retained name-identified information is expressly excluded from provisions for special access under s 56 of the *Archives Act* or by disclosure by National Archives of Australia staff, including to a court or tribunal.[67]

13.62 In relation to the SLCD, the ALRC acknowledges the serious concerns about the privacy risks associated with the development of a rich longitudinal dataset that related to the entire Australian population. The ALRC notes the concerns of stakeholders that

---

63 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Parliament of Australia—House of Representatives Legal and Constitutional Affairs Committee, *Saving Our Census and Preserving Our History* (1998), [4.10]–[4.14].

64 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

65 *Census and Statistics Act 1905* (Cth) s 8A.

66 National Archives of Australia, *Submission PR 199,* 20 February 2007.

67 *Archives Act 1983* (Cth) ss 22B, 30A.

such a dataset might appear too attractive for future non-statistical or administrative uses. The ALRC notes, however, that the modified proposal for the SLCD to be based on a 5% sample of the population will make the dataset much less attractive for other uses, including administrative and other non-statistical uses.

13.63 The ALRC acknowledges the privacy concerns that some members of the public have in the period leading up to the taking of the census. The ALRC is, however, satisfied that the legislative framework within which the ABS operates and conducts the census is privacy protective. The ABS is subject to the *Privacy Act* as well as confidentiality provisions under the *Census and Statistics Act*. Names and addresses are not retained for longer than the period required for census processing, and are used only in relation to census processing and for ABS quality studies. Names and addresses are destroyed at the end of census processing.[68]

13.64 Further, various administrative arrangements for the collection of census data are designed to protect the privacy of individuals participating in the census. For example, householders who do not wish other members of the household to see their information may request a personal census form. Those who are concerned about the census collector seeing the form can ask for a privacy envelope or can complete the census form online using the eCensus. Householders who still have concerns can ask the census collector for a reply-paid 'mailback' envelope to post their completed form directly to the ABS.[69]

Corporations Act 2001 (Cth)

13.65 Section 168 of the *Corporations Act 2001* (Cth) requires companies and registered schemes to maintain a register of members and, if relevant, a register of option holders and a register of debenture holders. Section 169 of the Act requires a register of members to contain certain details, including the member's name and address, the date on which the member's name was entered on the register, as well as other details such as the shares held by each member.

13.66 Under s 173 of the *Corporations Act*, companies, registered schemes and persons who maintain registers on behalf of companies and registered schemes must allow anyone to inspect these registers.[70] Section 173 of the Act is an example of a provision that requires or authorises the disclosure of information for the purposes of the *Privacy Act*. It is unlikely therefore that compliance with the *Corporations Act* requirements would breach NPP 2.

13.67 Section 177 of the *Corporations Act* provides that it is a criminal offence if a person uses information about a person obtained from a register to contact or send material to the person or disclose information of that kind knowing that the information

---

68 D Trewin (Australian Statistician), 'Census Data Enhancement Project—Statement of Intention' (Press Release, 18 August 2005).

69 See Australian Bureau of Statistics, *2006 Census: Privacy and Confidentiality* <www.abs.gov.au> at 31 July 2007.

70 *Corporations Act 2001* (Cth) s 173.

is likely to be used to contact or send material to the person. An exception to that rule is where the use of the information is connected with the membership, or approved by the company.

13.68 Link Market Service submitted that the provisions relating to access to registers under the *Corporations Act* are contrary to the NPPs.[71] It was noted that under the *Privacy Act*, a company that maintains a members register cannot provide personal information except for the primary purpose of managing a members register, and yet under the *Corporations Act* it is able to disclose information that would not usually be disclosed.

> Practically we cannot, for example, disclose information to a shareholder that calls in without providing their unique identifier (their Securityholder Reference Number) but can allow access to a register to a member of [the] public if they visit our offices to a view a register (in this process they can see a specific individual's holding balance).[72]

13.69 Particular concerns relating to mutual entities, such as credit unions, have also been raised. It has been argued that the personal information on a credit union's member register is more detailed and revealing than information on an ordinary company register,[73] and that access to this information will encourage misuse of this information.[74] Amendments have been made to the *Corporations Regulations 2001* (Cth) to deal with this issue.[75] Regulation 12.8.06 of the *Corporations Regulations* allows mutual entities to:

- have a separate register of 'member shares' being the shares which are issued by them to their customers;
- require the party seeking access to agree in writing that the information about members which is gained will be divulged only to certain named persons and used only for certain specified purposes; and
- refuse access if it is not satisfied that access is being sought by a member who intends to call a meeting of members, or for another purpose approved by the Australian Securities and Investments Commission (ASIC).

13.70 Further, the *Corporations Amendment Regulations 2007 (No 9)* (Cth) provide that when a person seeks access to a register of members of certain body corporates (a credit union, credit society and building society) and the person has given a statutory declaration in relation to the use of that information and paid the reasonable costs of contacting the members, or sending material to the members, the body corporate must

---

71 Link Market Service, *Submission PR 2,* 24 February 2006.

72 Ibid.

73 See Information Integrity Solutions, *Customer Lists: Background Paper for CUSCAL Industry Association* (2005).

74 Credit Union Industry Association and others, *Issues Overview: Member Registers, Takeovers and Mutuals* (2006).

75 *Corporations Amendment Regulations 2003* (Cth).

do everything that is reasonably possible to arrange for the members to be contacted, or for the material to be sent to the members, on the person's behalf by a third party service provider nominated by the body corporate.

Submissions and consultations

13.71 In IP 31, the ALRC asked whether it is appropriate that the disclosure of a shareholder's personal details in a register of members, register of debenture holders or a register of option holders under the *Corporations Act* is a disclosure of personal information that is permitted for the purposes of NPP 2.[76]

13.72 One stakeholder submitted that such disclosure is appropriate and clearly permitted for the purposes of NPP 2.

> The law imposes this obligation on companies for good reasons. The members and directors of a company have the considerable advantage of limited liability. That means that persons dealing with the company cannot generally proceed against its members or directors for debts owed to them by the company. There is a concomitant obligation that goes with that benefit, and that is that those members and directors must be prepared to disclose that they control or have an interest in the company.[77]

13.73 The submission noted that the *Corporations Act* imposes criminal penalties for inappropriate use of information held on a register. It was also observed that there are a number of legitimate reasons why someone might wish to obtain membership details. For example, a member or third party may seek to circulate material to members of the company raising issues about the performance of the company or its management; a member may seek to convene a general meeting of the members; and a member or third party may make a bid for securities held by the members of the company.[78] It was submitted that access to personal information for these reasons facilitates informed dealings by members, prospective members and other stakeholders, which is conducive to the good governance of a company.

> The law does not prohibit inspection of registers because some people might, conceivably, abuse the privilege. It leaves the privilege open to all, with sanctions for misuse. Transparency of ownership and accountability are, if you like, the 'costs' which necessarily go with the benefit of limited liability. These are some of the necessary consequences of choosing to do business by means of a company.[79]

13.74 The ALRC also heard a number of concerns about the disclosure of shareholder's personal details in a register of members. The OPC noted community concern regarding access to share registers, particularly where information derived from registers is used for purposes that shareholders may not expect. The OPC has received complaints and enquiries about share register information being used to make unsolicited purchase offers to individuals, including at opportunistic prices; concerns that shareholding registers may reveal information about the financial wealth of an

---

76 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(j).
77 Confidential, *Submission PR 165,* 1 February 2007.
78 Ibid.
79 Ibid.

individual; and information being used for unsolicited direct marketing.[80] The OPC submitted that it may be appropriate to describe more carefully the range of permitted uses and disclosures of this data.[81]

13.75 A number of issues were raised in relation to personal information held on a credit union's member register. The National Credit Union Association (NCUA) stated that the majority of customers of credit unions are individuals, which is in contrast to listed companies, which will generally have a greater number of corporate shareholders. This has significant ramifications for a credit union, as disclosure of the shareholder register is a disclosure of a credit union's client base, which comprises mostly persons, not corporations.[82]

13.76 The NCUA also noted that credit unions are often structured to service particular groups of people, which are characterised by community, locality or some element of workplace or professional association or ethnic origin. In the view of NCUA, the fact that a person is on the shareholders' register of a credit union may indicate that person's racial or ethnic origin or professional association, which may amount to sensitive information. NCUA submitted that it should be of concern to government that any person may obtain the names, addresses and other details of police, military personnel, pilots and teachers who are members of specific industry-based credit unions.[83]

13.77 Abacus–Australian Mutuals (Abacus) welcomed the recognition of the different status of mutual member registers provided in the *Corporations Regulations*, but submitted that a 'clear mailing house' was required. Under the model, where lawful contact was to occur with members of a mutual this would be conducted at 'arm's length' with material managed by a professional mailing house or some other trusted third party, ensuring that member information is not required to be released to the applicant.[84]

13.78 Abacus observed an increased interest in the launching of takeovers and demutualisations of mutual entities. Rather than pursuing these as formal takeovers, third parties have, in some cases, sought to advance their proposals by direct lobbying of members (for example, seeking to have boards directed to take action or to replace directors with a pro-demutualisation board).[85]

---

80 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also H Walker, *Submission PR 55,* 20 October 2006.

81 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

82 National Credit Union Association Inc, *Submission PR 226,* 9 March 2007. See also Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

83 National Credit Union Association Inc, *Submission PR 226,* 9 March 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

84 This submission was received prior to the promulgation of the *Corporations Amendment Regulations 2007 (No 9)* which provides for a mailing house option.

85 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

13.79 Abacus also noted that ASIC has used its approval powers under the *Corporations Regulations* to authorise the release of mutual register information to third parties (in some instances, direct competitors) who are seeking to launch informal takeovers and demutualisations without imposing protections covering member information or ensuring strong disclosure rules were in place.[86]

13.80 One submission noted, however, that the content requirements for registers of members apply to companies which conduct a credit union business in the same way as they apply to all other companies. It was also noted that credit unions have the benefit of further controls on the use to which such information may be put. It was submitted that these further controls represent substantial advantages which are not enjoyed by companies generally and should promote the bona fide use of the registers of members of credit union companies.[87]

ALRC's view

13.81 The ALRC does not make a proposal in relation to the use and disclosure of personal information held on a register of members. In the ALRC's view, the *Corporations Act* provides significant protection of personal information held on a register. These protections strike the appropriate balance between the right of the public to know about, and use, information from the register, and the policy that shareholders should be free from undue intrusion from the use of such information. The ALRC also notes that the member registers of mutuals, such as credit unions, receive extra protection under the *Corporations Regulations* as amended by the *Corporations Amendment Regulations 2007 (No 9)*, which provide for the use of a mailing house when a third party seeks access to a credit union's register of members.

13.82 The *Privacy Act* also provides some protection for personal information held on a members register.[88] For example, the collection by an organisation of information from a register will be subject to NPP 1. Personal information included on a register is subject to the data quality requirements of NPP 3. The application of the *Privacy Act* to publicly available information is discussed further in Chapter 8.

Commonwealth Electoral Act 1918 (Cth)

13.83 The *Commonwealth Electoral Act 1918* (Cth) and the *Privacy Act* provide the legislative privacy framework governing the electoral roll. Part VI of the *Commonwealth Electoral Act* provides for the establishment of an electoral roll. Under s 101 of the Act it is compulsory for all eligible persons in Australia to maintain continuous enrolment on the Commonwealth electoral roll for the purposes of federal elections and referendums. The names and addresses of all electors on the Commonwealth electoral roll are available for public inspection in various formats specified under the *Commonwealth Electoral Act*.[89] The Act also requires the provision

86 Ibid.
87 Confidential, *Submission PR 165,* 1 February 2007.
88 *Privacy Act 1988* (Cth) s 16B.
89 *Commonwealth Electoral Act 1918* (Cth) ss 90, 90A.

of electoral roll information to a number of different individuals and organisations, including members of Parliament and political parties.[90]

13.84 Section 91A of the *Commonwealth Electoral Act* provides that a person or organisation that obtains information under s 90B must not use it except for a permitted purpose. The permitted purposes in relation to a political party include: any purpose in connection with an election or referendum, research regarding electoral matters, and monitoring the accuracy of information contained in a roll. Disclosure to political organisations for these permitted purposes would constitute a secondary purpose that is authorised by law for the purposes of the *Privacy Act*.[91]

13.85 One issue for consideration is whether the provisions under the *Commonwealth Electoral Act* and the *Privacy Act* provide adequate protection for personal information—particularly information provided to political organisations. Although the *Commonwealth Electoral Act* regulates what electoral roll information can be provided to individuals and organisations, and how they can use the information, it does not provide for other information privacy protection such as in relation to data security and retention. These issues are dealt with in the NPPs. The NPPs do not, however, apply to acts or practices carried out by political organisations and their contractors, subcontractors and volunteers in relation to electoral matters.[92] Issues related to the political exemption are discussed in detail in Chapter 37.[93] Privacy concerns related to developments in technology and the use of public registers such as the electoral roll are discussed in Chapter 8.

Submissions and consultations

13.86 It was submitted that protection consistent with the principles contained in the *Privacy Act* should be afforded to the handling of information from the electoral roll, particularly in regard to those bodies that may handle such information but which are not regulated under the *Privacy Act*.[94] The OPC submitted that consideration should be given to extending the types of protections that are afforded under the *Commonwealth Electoral Act*, including by introducing obligations to ensure that recipients handle information securely and dispose of it when it is no longer required for the purpose for which it was collected.[95]

13.87 A number of submissions noted that amendments to the *Commonwealth Electoral Act* have resulted in the electoral roll being used for a purpose other than the primary purpose for which the personal information was collected. In particular, it was

---

90 Ibid s 90B.
91 *Privacy Act 1988* (Cth) s 14, IPP 10.1(c).
92 Ibid s 7C.
93 In Ch 37, the ALRC proposes substantial amendments to the political exemption. See Proposals 37–1, 37–2.
94 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
95 Ibid.

submitted that the electoral roll is now a resource for identity management.[96] This is particularly the case in relation to the new obligations under the AML/CTF Act.

13.88 The OPC reported concerns in the community about the use of information sourced from old electoral rolls, in particular for direct marketing. The OPC also noted concern about the alleged use of information on the electoral roll by debt collectors. In one case, a debt collector, acting on behalf of a psychiatrist, allegedly sent an account on the psychiatrist's letterhead to the debtor's work address. In another case, a debt collector allegedly sent letters of demand to all persons of the same name listed on the electoral roll in an attempt to recover a debt.[97]

13.89 There was, however, some support for greater access to the electoral roll. The Institute of Mercantile Agents submitted that:

> The current senseless banning of the release of Electoral Roll information is costing consumers over $4Billion in unlocated accounts—again the cost of those debts are passed on: those who pay, pay extra for those who don't! Despite holding an individual's consent to use electoral roll information. Such information should also be a privacy requirement of credit bureaux to assist in holding correct information.[98]

13.90 The OPC noted the range of agencies that are able to access the electoral roll. Under the *Electoral and Referendum Regulations 1940* (Cth), 22 Australian Government agencies are authorised to access information on the electoral roll for a range of regulatory, law enforcement and public revenue purposes.[99] In the OPC's view, given the mandatory nature of enrolment, it is appropriate that access to the electoral roll remain relatively narrow.[100]

13.91 Stakeholders also expressed concern about the use of information from other agencies to update the roll. Under s 92 of the *Commonwealth Electoral Act*, the Australian Electoral Commission has substantial powers to collect personal information from a range of Australian Government and state and territory agencies to maintain the integrity of the electoral roll. Updating the roll would include, for example, matching personal information from another source with the personal information held on the electoral roll. The OPC submitted that:

> In the context of the Electoral Roll, it may be appropriate that any data-matching only be pursued where appropriate regard for privacy issues has been given. In particular, the purpose of the data-matching should be narrowly defined as being to maintain the accuracy of the Electoral Roll. Further, formal protocols may be required to ensure that redundant or unmatched personal information is not retained.[101]

13.92 The OVPC noted that a tension arises when the Australian Electoral Commission demands bulk access to personal information held by state electoral

---

96 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
97 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
98 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
99 *Commonwealth Electoral Act 1918* (Cth) sch 1.
100 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
101 Ibid.

authorities in order to verify the identity of voters. The OVPC submitted that, in principle, state authorities are the 'best custodians' of these datasets.[102]

ALRC's view

13.93 The compulsory provision of information for the electoral roll requires that an appropriate balance be struck between the public interest in ensuring transparent electoral procedures and the public interest in protecting privacy. In the ALRC's view, the *Commonwealth Electoral Act* and the *Privacy Act* balance these interests appropriately.

13.94 The ALRC is concerned, however, that, due to the interaction between the *Commonwealth Electoral Act* and the exemptions under the *Privacy Act*, political organisations and their contractors, subcontractors and volunteers are not subject to any rules relating to secure storage and retention of personal information held on the electoral roll. The ALRC notes that the secure storage and destruction of this information is essential to guard against unauthorised use of old electoral rolls for purposes such as direct marketing.

13.95 This will no longer be an issue if the exemption under the *Privacy Act* that applies to registered political parties and political acts and practices is removed as proposed.[103] In the event that it is not, the ALRC proposes that the *Commonwealth Electoral Act* should be amended to provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information in relation to the electoral roll and certified lists of voters must take reasonable steps to:

- protect the information from misuse and loss and from unauthorised access, modification or disclosure; and
- destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.

13.96 The primary purpose of collection of personal information for inclusion in the electoral roll is to produce and maintain an accurate record of those who are entitled to vote, thus minimising electoral fraud and promoting the participation of all eligible citizens in the democratic process.

13.97 The electoral roll is being used increasingly for purposes other that the primary purpose, such as for complying with obligations under the AML/CTF Act. The ALRC is, however, conscious that these secondary uses are required or authorised by law, and that there is a need for access to personal information in order to comply with statutory identity verification requirements.

13.98 In the ALRC's view, the OPC should continue to monitor the use of the electoral roll for other than electoral purposes. The ALRC proposes below that the

---

102 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
103 See Ch 37.

seven year statutory review of the AML/CTF Act consider a variety of matters.[104] The ALRC considers that this review should also consider whether use of the electoral roll for the purposes of identity verification under the AML/CTF Act continues to be appropriate.

13.99 The ALRC acknowledges concerns in relation to data-matching to update the roll and the retention of redundant or unmatched personal information. In the ALRC's view, the Australian Electoral Commission and state and territory electoral commissions, in consultation with the OPC, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

Proposal 13–1 If the exemption that applies to registered political parties and political acts and practices is not removed, the *Commonwealth Electoral Act 1918* (Cth) should be amended to provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information in relation to the electoral roll and certified lists of voters must take reasonable steps to:

(a) protect the information from misuse and loss and from unauthorised access, modification or disclosure; and

(b) destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.

Proposal 13–2 The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

13.100 The AML/CTF Act received Royal Assent on 12 December 2006. It is intended to enable individual businesses to manage money laundering and terrorism financing risks. The Act sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person who provides 'designated services'.[105] A large number of 'designated services' are listed in the Act including opening an account, making a loan, and supplying goods by way of hire purchase.[106]

104 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 251.
105 Ibid s 5.
106 Ibid s 6.

13.101 The Act requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer.[107] In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters,[108] and must develop and comply with an anti-money laundering and counter-terrorism financing program.[109] The Act also imposes various record-keeping requirements on reporting entities.[110] For example, a reporting entity must make a record each time it provides a designated service and must retain the record for seven years.[111]

13.102 Part 11 of the Act relates to secrecy and access. Except as permitted by the Act, certain individuals including an AUSTRAC official, a customs officer or a police officer must not disclose information or documents obtained under the Act.[112] Further, a reporting entity must not disclose that it has reported, or is required to report, information to AUSTRAC; or that it has formed a suspicion about a transaction or matter. The Part also provides that the Australian Taxation Office and certain other 'designated agencies' may access AUSTRAC information. The term 'designated agencies' is defined in s 5 to include a large number of Australian Government agencies as well as some state and territory agencies. Designated agencies may access AUSTRAC information for the purposes of performing that agency's functions and exercising the agency's powers.[113] The Act requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of the accessed AUSTRAC information.[114]

Background

13.103 The AML/CTF Act is the result of an extensive consultation process. On 16 December 2005, the Government released the exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill (the exposure Bill) along with draft Rules.[115] The Australian Government Attorney-General's Department received 120 submissions on the exposure Bill. The exposure Bill was referred to the Senate Legal and Constitutional Legislation Committee. The Committee reported on its inquiry on 13

107 Ibid pt 2.
108 Ibid pt 3.
109 Part A of an anti-money laundering and counter-terrorism financing program is a program that is designed to identify, mitigate and manage the risk a reporting entity may reasonably face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism. Part B of an anti-money laundering and counter-terrorism financing program sets out the applicable customer identification procedures for customers of the reporting entity: Ibid s 80.
110 Ibid pt 10.
111 Ibid s 107.
112 Ibid pt 11, div 2.
113 Ibid s 126.
114 Ibid s 126(3).
115 See Australian Government Attorney-General's Department, *Anti-money Laundering* <www.ag.gov.au> at 30 July 2007.

April 2006.[116] The Committee concluded that an independent privacy impact assessment of the Bill should be conducted. The Committee also recommended that the Bill should contain a statement that is reflective of the intention to allow federal, state and territory agencies to access and utilise AUSTRAC data for purposes that may not be related to anti-money laundering or counter-terrorism financing, such as detecting tax and social security fraud.[117]

13.104 The Australian Government Attorney-General's Department released a revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (revised AML/CTF Bill 2006) and draft Rules for a further period of consultation which ended on 4 August 2006.[118] The Department received a further 70 submissions on the revised AML/CTF Bill 2006. Submissions in response to the revised AML/CTF Bill 2006 raised a number of privacy issues.

13.105 In September 2006, an independent privacy impact assessment was conducted. The privacy impact assessment made 96 recommendations. Key recommendations were that:

- The scheme should be proportionate to the risk. It was suggested that some aspects of the proposal are overly intrusive into people's personal affairs compared with the current risks posed by money laundering and terrorism financing.
- The use of personal information should be limited to the stated objectives of the scheme. There were significant concerns about the collection, use, and disclosure of personal information for purposes which were deemed to be unrelated to the objectives of tackling money laundering and terrorism financing (eg, use by government agencies such as ASIC, Centrelink and the Australian Competition and Consumer Commission).
- The NPPs should be extended to all reporting entities. Many reporting entities and government agencies will not be subject to privacy obligations in the collection and use of personal information by virtue of legislative limitations. It was suggested that reporting entities under the Bill could be subject to the NPPs by amending the *Privacy Act* for the purposes of AML/CTF compliance. Where no or limited privacy obligations exist for government agencies, the Bill could also be amended to ensure that these agencies are subject to Commonwealth jurisdiction as a condition of receiving AUSTRAC information.[119]

116 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (2006).
117 Ibid, [4.72]–[4.76].
118 Revised Exposure Draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth).
119 Salinger & Co, *Privacy Impacts of the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules* (2006).

13.106 The Australian Government published a Privacy Impact Statement which responded to the PIA findings and recommendations. The Government adopted 30 of the 96 recommendations.[120]

13.107 The final version of the Anti-Money Laundering and Counter-terrorism Financing Bill 2006 (Cth) (AML/CTF Bill 2006) was introduced in the Parliament on 1 November 2006. The final version of the Bill required that designated agencies, including state and territory agencies, comply with the IPPs in respect of the accessed AUSTRAC information.

13.108 After its introduction, the AML/CTF Bill was referred to the Senate Legal and Constitutional Legislation Committee. Submissions to the Senate Committee continued to raise privacy issues. The Committee reported on its inquiry on 28 November 2006. The Committee recommended that the Australian Government consider amending the Bill to include further threshold value limits, to exclude low risk, low value services (such as the provision of travellers cheques and foreign currency transactions) from the definition of 'designated services' and that consideration be given to indexing these thresholds every five years. The Committee also recommended that the OPC conduct periodic audits of AUSTRAC's compliance with privacy obligations in its administration of the Bill.[121]

13.109 The *Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006* (Cth) was assented to on the same day as the AML/CTF Act. The *Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act* introduced s 63(1A) into the *Privacy Act.* This provision has the effect of classifying a small business operator that is a reporting entity (a person who provides a designated service under the AML/CTF Act) to be an organisation for the purposes of the *Privacy Act*, ensuring that all reporting entities are subject to the *Privacy Act* in relation to their obligations to collect personal information under the AML/CTF Act.

Submissions and consultations

13.110 Submissions raised a number of issues in relation to the AML/CTF Act. The Australian Privacy Foundation submitted that privacy was not adequately protected under the anti-money laundering and counter-terrorism laws.

> The AML-CTF legislation, now passed, represents one of the most objectionable and disproportionate intrusion into financial privacy, as well as extending the existing

120 Australian Government Attorney-General's Department, *Privacy Impact Statement: Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules* (2006).

121 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]* (2006). None of these recommendations have been implemented to date.

> system of highly subjective suspect transaction reports, which are exempt from access and correction rights.[122]

13.111 The OVPC submitted that there is a significant risk that the proposed measures will lead to pervasive monitoring of the financial affairs of ordinary citizens—not necessarily due to any suspicion that they are financiers of terrorism or money launderers, but simply by virtue of their engaging in what may be ordinary everyday transactions.[123]

13.112 The OPC also referred to its previous submissions in relation to the anti-money laundering and counter-terrorism laws. The key concerns raised in these submissions about the various iterations of the Bill included that:

- state and territory agencies may access information collected by AUSTRAC without being subject to the same accountability under the *Privacy Act* as Australian Government agencies;
- designated partner agencies have been granted access to AUSTRAC data using information for purposes outside of the intentions of anti-money laundering and counter-terrorism financing;
- the $10,000 mandatory reporting thresholds for reporting need to be reviewed to reflect price inflation and minimise the unnecessary collection of personal information; and
- the AML/CTF Act sits uncomfortably with the general privacy principle that individuals should be able to interact anonymously wherever practical.[124]

13.113 Concern was expressed in a number of submissions that designated agencies have been granted access to AUSTRAC data to use for purposes other than those of anti-money laundering and counter-terrorism.[125] Submissions also observed that the 'safeguard' under s 126(3) of the AML/CTF Act requiring state and territory government agencies recipients to agree to comply with the IPPs in the *Privacy Act* is of limited value, given the lack of enforceable remedies for any breaches, and an

---

122 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

123 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007 referring to Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, 17 November 2006.

124 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

125 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007 referring to Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, 17 November 2006.

inability to investigate those agencies.[126] It was also noted that the AML/CTF Act does not take into account existing state and territory privacy laws.[127]

13.114 Access and the limitations on that access to AUSTRAC information is controlled by an Instrument of Authorisation signed by the AUSTRAC Chief Executive Office under s 126(1) of the AML/CTF Act, together with a memorandum of understanding (MOU) between the AUSTRAC Chief Executive Officer and the chief executive of each of the 29 designated agencies with whom AUSTRAC has signed an MOU.

13.115 AUSTRAC stated that online access is restricted to officials who need to access reports online. Access to suspect transaction reports is limited, and AUSTRAC maintains audit trails of access by its own staff, by the Australian Taxation Office and by designated agency officers. Other submissions noted, however, that it is not appropriate that obligations to protect personal information be left to the discretion of the AUSTRAC Chief Executive Officer, and that it would be more appropriate for Parliament to determine the appropriate safeguards that should apply.[128]

13.116 Submissions noted that the record-keeping provisions in the Act generally require reporting entities to retain information for up to seven years. The OPC and others have stated that any retention period should be determined with reference to the policy intent of NPP 4.2 which requires that personal information should be destroyed once it is no longer needed for any purposes for which it may be used or disclosed under NPP 2.[129]

13.117 A number of submissions from financial institutions and peak industry bodies noted that the AML/CTF Act requires a reporting entity to carry out a procedure to verify a customer's identity prior to providing a designated service, but does not

---

126 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007 referring to Australian Privacy Foundation, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, 17 November 2006.

127 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007 referring to Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, 17 November 2006.

128 Ibid.

129 Office of the Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, November 2006; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007 referring to Australian Privacy Foundation, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 [Provisions] and Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Bill 2006 [Provisions]*, 17 November 2006.

expand access to available databases for identity verification purposes.[130] Some submissions raised the issue of using credit reporting information for the purposes of identity verification. This issue is discussed in Chapter 53.

ALRC's view

13.118 There have been a number of recent inquiries that have considered the AML/CTF Act. The ALRC, therefore, restricts its consideration of the Act to issues raised in submissions to this Inquiry. The ALRC shares many of the concerns raised by stakeholders in relation to the AML/CTF Act. In particular, the ALRC is concerned about the pervasive nature of the monitoring that is to occur due to the mandatory reporting threshold remaining at $10,000. As suggested by the OPC, the threshold should be reviewed to reflect price inflation and minimise the unnecessary collection of personal information.

13.119 The provisions requiring reporting entities to retain information for seven years are inconsistent with NPP 4.2 which requires that personal information should be destroyed once it is no longer needed for any purpose for which it may be used or disclosed. The ALRC is conscious, however, that there may be circumstances where this information will need to be retained for seven years in order to assist an investigation into anti-money laundering or counter-terrorism financing.

13.120 Under s 251 of the AML/CTF Act, the Minister must cause a review to be conducted of the operation of the Act, the regulations and the AML/CTF Rules before the laws have been in operation for seven years. This review should consider whether reporting entities and designated agencies are handling personal information appropriately under the legislation.

13.121 The review should also examine whether the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation; and whether it remains appropriate that reporting entities are required to retain information for seven years. The ALRC also proposes that the review of the AML/CTF Act consider whether it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.

13.122 The ALRC is concerned about the number of designated agencies that have been granted access to AUSTRAC data collected under the AML/CTF Act, and the limited protection offered by s 126(3) of the Act. In the ALRC's view, due to the amount of personal information that will be made available to the agencies, it is appropriate that these agencies should have to comply with the IPPs under the *Privacy Act* in relation to that information. While the agencies must agree to be bound by the IPPs, the Privacy Commissioner does not have the power to audit or enforce compliance with the IPPs by state and territory agencies.

---

130 ING Bank, *Submission PR 230,* 9 March 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

13.123 The ALRC proposes that the AML/CTF Act should be amended to provide that state and territory agencies that access personal information provided to AUSTRAC be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act.*

13.124 The ALRC acknowledges that there may be some opposition to this proposal from state and territory governments.[131] The ALRC notes, however, that its proposal would extend the application of the *Privacy Act* to state and territory agencies only in relation to the information provided to AUSTRAC pursuant to the AML/CTF Act; and where the state and territory agencies are not covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act.*[132] Further consultation with state and territory governments is required.

Proposal 13–3 The review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), the regulations and the Anti-Money Laundering and Counter-Terrorism Financing Rules under s 251 of the Act should consider, in particular, whether:

(a) reporting entities and designated agencies are appropriately handling personal information under the legislation;

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years; and

(d) it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.

131 The Australian Parliament's power under the *Australian Constitution* to legislate in relation to the handling of personal information by state and territory public sectors is discussed in Ch 4.

132 In Ch 4, the ALRC proposes that states and territories should enact privacy laws to regulate that state or territory's public sector that apply the proposed Unified Privacy Principles and the proposed *Privacy (Health Information) Regulations* as in force under the *Privacy Act* from time to time. The ALRC has also proposed that the Australian Government should initiate a review in five years to consider whether the proposed Commonwealth-state cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors. See Proposals 4–4 and 4–5.

Proposal 13–4 The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should be amended to provide that state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the Act be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act.*

14. Interaction with State and Territory Laws

Contents

Introduction 519
Interaction of federal, state and territory regimes 519
Scope of federal, state and territory regimes 520
Personal information regulated 523
Inconsistent principles 523
Regulators 524
Remedies 525
State and territory legislation adopting *Privacy Act* provisions 525
Privacy rules, codes and guidelines 526
Submissions and consultations 527
ALRC's view 528
Residential tenancy databases 528
Submissions and consultations 531
ALRC's view 534

Introduction

14.1 This chapter considers how the *Privacy Act 1988* (Cth) interacts with state and territory privacy laws. The chapter first identifies a number of examples of inconsistency between the *Privacy Act* and privacy regimes that regulate state and territory public sectors. The chapter then examines inconsistency and fragmentation in privacy rules, codes and guidelines. The final section of the chapter considers the regulation of residential tenancy databases. A number of inquiries have now recognised the need for national consistency in the regulation of residential tenancy databases.

Interaction of federal, state and territory regimes

14.2 In the absence of a clear statement in the *Australian Constitution* about whether the regulation of personal information is the responsibility of the Australian Government or state and territory governments, the states and territories are able to enact privacy laws.[1] Further, s 3 of the *Privacy Act* states that the Australian Parliament does not intend to 'cover the field' in relation to the protection of personal information.[2] Chapter 2 provides an overview of state and territory privacy laws.

---

1 The Constitutional basis for enacting the *Privacy Act 1988* (Cth) was the Australian Government's power to make laws in relation to 'external affairs': *Privacy Act 1988* (Cth) Preamble; *Australian Constitution* s 51(xxix).

2 *Privacy Act 1988* (Cth) s 3 and the *Australian Constitution* are discussed in Ch 4.

14.3 State and territory laws are sometimes inconsistent with the *Privacy Act* and with each other. Legislation regulates personal information at the federal level and in New South Wales, Victoria, Tasmania, the ACT and the Northern Territory.[3] Queensland and South Australia have adopted administrative regimes for the management of personal information in their state public sectors.[4] Western Australia does not have a legislative scheme to regulate the handling of personal information; state freedom of information legislation and public records legislation provides some privacy protection.[5] On 28 March 2007, the Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information by the public and private sectors in Western Australia.

14.4 Further, legislation in New South Wales, Victoria and the ACT regulates health information in the public and private sectors.[6] These Acts overlap substantially with the private sector provisions in the *Privacy Act*. Regulation of health information in other jurisdictions is restricted to public sector agencies or is the subject of non-legislative codes and guidelines.[7] Inconsistency and fragmentation in health privacy regulation is discussed in Part H.

Scope of federal, state and territory regimes

State-owned corporations

14.5 The *Privacy Act* exempts state and territory authorities from the operation of the *Privacy Act*[8] unless the states and territories request that such authorities be brought into the regime by regulation.[9] State instrumentalities are subject to the private sector provisions of the Act, unless they have been prescribed to fall outside the definition of 'organisation'.[10]

---

3 *Privacy Act 1988* (Cth); *Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW); *Information Privacy Act 2000* (Vic); *Health Records Act 2001* (Vic); *Personal Information Protection Act 2004* (Tas); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act 2002* (NT).

4 Queensland Government, *Information Standard 42—Information Privacy* (2001); Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001); South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

5 *Freedom of Information Act 1992* (WA); *State Records Act 2000* (WA).

6 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

7 For further discussion see Ch 2 and Part H.

8 *Privacy Act 1988* (Cth) s 6C. The expression 'state or territory authority' includes persons and bodies which form part of state or territory governments and bodies established under state or territory laws or by the executive branches of state or territory governments.

9 Ibid s 6F.

10 Ibid ss 6C(4), 6F. An instrumentality of a state or territory includes a state or territory government business enterprise: see Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15751 (D Williams—Attorney-General); M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.71].

14.6 While a number of state and territory privacy regimes regulate the handling of personal information by state-owned corporations,[11] they are not regulated in New South Wales. This is significant as state-owned corporations do not fall within the ambit of the private sector provisions of the *Privacy Act* unless they are prescribed by regulation.[12]

14.7 The exemptions under the *Privacy Act* relating to state and territory authorities and prescribed instrumentalities are discussed further in Chapter 34. In that chapter, the ALRC proposes that the *Privacy Act* be amended to apply to all state and territory incorporated bodies, including statutory corporations, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act.*

State contracted service providers

14.8 There is also confusion about whether contracted service providers to New South Wales government agencies are caught by the *Privacy Act* or the *Privacy and Personal Information Protection Act 1998* (NSW), or fall into an unregulated gap between the state and federal Acts.[13] In Chapter 11, the ALRC discusses various issues related to state contracted service providers. In Chapter 4, the ALRC proposes that state and territory legislation regulating the handling of personal information in that state or territory's public sector should include provisions relating to state and territory government contracts.

Ministers, local governments and universities

14.9 While legislation in some jurisdictions applies to ministers,[14] the *Privacy and Personal Information Protection Act 1998* (NSW) does not cover ministers and specifically authorises the disclosure of information to ministers and the Premier.[15] The handling of personal information by local governments is regulated under privacy regimes in some states and territories.[16] Local governments are not regulated, however, in Queensland[17] or South Australia.[18]

---

11 See, eg, *Information Privacy Act 2000* (Vic) s 3; Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

12 *Privacy Act 1988* (Cth) s 6C(1).

13 See Ibid s 7B(5); *Privacy and Personal Information Protection Act 1998* (NSW) s 4(4)(b); Privacy NSW, *Submission to the New South Wales Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998*, 24 June 2004, 77.

14 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.

15 *Privacy and Personal Information Protection Act 1998* (NSW) s 28(3).

16 For example, Ibid s 3; *Information Privacy Act 2000* (Vic) s 9(1)(d).

17 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1] and *Financial Management Standard 1997* (Qld) s 5(2)(c).

18 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), 2(2) and *Public Sector Management Act 1995* (SA) s 3.

14.10 Further, universities are subject to personal information laws in some jurisdictions,[19] but not others.[20] Most universities are established under state or territory legislation and will therefore generally be exempt from the *Privacy Act*. If there is no privacy legislation in the jurisdiction in which they are established, then how they handle personal information may not be regulated. Universities handle substantial amounts of personal information.[21] Private universities and universities established under ACT legislation are covered by the *Privacy Act*, as are other private sector higher education providers. This creates further inconsistency in privacy regulation between bodies that substantially provide the same function.[22]

14.11 The ALRC proposes that the states and territories enact legislation that applies the proposed Unified Privacy Principles (UPPs) and the Privacy (Health Information) Regulations.[23] This legislation should include a definition of 'agency' that includes ministers, universities, and local governments. This will ensure that these individuals and agencies are subject to the same privacy principles.

Intergovernmental bodies

14.12 In its submission to the Inquiry, the OPC submitted that:

> The existing definition for 'agency' in the *Privacy Act* may benefit from additional clauses to clarify currently ambiguous areas of coverage. In particular, coverage of some public authorities created as collaborations between the Commonwealth and the States and Territories by the Council of Australian Governments (COAG) and other Ministerial Councils could be better provided for under the definition of agency in the *Privacy Act*.[24]

14.13 The ALRC notes that bodies established by cooperative arrangements, such as intergovernmental working groups and officer working groups that assist ministerial councils, may often have to share personal information. The application of privacy regulation to such entities will often be uncertain, as they may not fall within the *Privacy Act* definition of organisation or agency, though equally they may not be considered state and territory agencies for the purpose of privacy regulation in other jurisdictions.

14.14 To ensure the protection of personal information held by Australian Government agencies, the ALRC proposes that the *Privacy Act* be amended to provide that when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies, the Australian Government agency should ensure that a memorandum of understanding is in place so that the

---

19 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.

20 See, eg, South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992), 2(2) and *Public Sector Management Act 1995* (SA) s 3.

21 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; D Antulov, *Submission PR 14,* 28 May 2006.

22 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

23 See Ch 4.

24 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

intergovernmental body and its members do not act, or engage in a practice, that would breach the Act.

Proposal 14–1 The *Privacy Act* should be amended to provide that when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies, the Australian Government agency should ensure that a memorandum of understanding is in place so that the intergovernmental body and its members do not act, or engage in a practice, that would breach the Act.

Personal information regulated

14.15 Employee records are excluded from the operation of the *Privacy Act*.[25] Some state and territory privacy regimes provide limited protection for employee records.[26] The Personal Information Protection Principles under the *Personal Information Protection Act 2004* (Tas) provide the highest degree of protection of employee records, subject to a number of exceptions.[27] In Chapter 36, the ALRC proposes that the current exemption under the *Privacy Act* relating to employee records should be removed. It is the ALRC's view that state and territory legislation should include provisions that address the handling of employee records in that state or territory's public sector.

14.16 The *Privacy Act* provides limited protection for information held in public registers. Information Privacy Principle 1 places some restrictions on the collection of personal information in a generally available publication.[28] Similarly, the *Information Act 2002* (NT) provides limited protection for information held in public registers.[29] Other jurisdictions, however, provide greater protection. For example, public registers in Victoria are subject to the Information Privacy Principles under the *Information Privacy Act 2000* (Vic),[30] and the New South Wales legislation prohibits certain disclosures of personal information held in a public register.[31] The issue of publicly available information is discussed in Chapter 3 and Chapter 8.

Inconsistent principles

14.17 Although the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) and privacy principles under state and territory privacy regimes are

25 *Privacy Act 1988* (Cth) s 7B(3).
26 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(j); M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005).
27 *Personal Information Protection Act 2004* (Tas) s 10.
28 Similar protection is offered under the Queensland Government, *Information Standard 42—Information Privacy* (2001), [3.1.1].
29 *Information Act 2002* (NT) s 68.
30 *Information Privacy Act 2000* (Vic) s 16(4).
31 *Privacy and Personal Information Protection Act 1998* (NSW) pt 6.

similar, they are not identical. The privacy regimes in some jurisdictions include privacy principles that are similar to the IPPs, while other jurisdictions have modelled their principles on the NPPs.[32] As is noted in Chapter 15, there are significant differences between the IPPs and the NPPs.

14.18 Many of the differences between the IPPs and the NPPs are reproduced in the state and territory regimes. For example, like the NPPs, the Information Privacy Principles under the *Information Privacy Act 2000* (Vic) include principles relating to anonymity and transborder data flows.[33] The Information Standard that applies to the Queensland public sector does not provide for either of these principles,[34] but the Information Standard that applies to the Queensland Department of Health does.[35]

14.19 The adoption of the proposed UPPs and Privacy (Health Information) Regulations at the federal, state and territory level will deal with many of the problems caused by inconsistent privacy principles across the jurisdictions.

Regulators

14.20 The nature and functions of privacy regulators vary across the jurisdictions. The *Privacy Act* and other federal legislation provide the Privacy Commissioner with a number of powers and functions, including powers to investigate and conciliate complaints, and approve and monitor privacy codes and guidelines.[36] Most states and territories have privacy regulators, but their nature and functions vary widely. For example, New South Wales and Victoria have full-time privacy regulators with a similar range of powers and functions to those of the federal Privacy Commissioner.[37] The Privacy Committee of South Australia's powers and functions, however, are limited compared to the federal, New South Wales and Victorian privacy commissioners.[38] Some jurisdictions, such as Tasmania and the Northern Territory, have regulators with functions other than oversight of the regulation of personal information.[39]

14.21 In Chapter 4, the ALRC notes that the proposed state and territory privacy legislation regulating the public sector should accommodate existing complaint and enforcement mechanisms. It is the ALRC's view, however, that when the states and territories enact these laws they should consider the establishment of a privacy regulator with similar functions and powers as the Privacy Commissioner.

---

32 See discussion in Ch 2.
33 *Information Privacy Act 2000* (Vic) sch 1.
34 Queensland Government, *Information Standard 42—Information Privacy* (2001).
35 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001), [3.1.8], [3.1.9].
36 See Part F for a discussion of the powers and functions of the Privacy Commissioner.
37 See discussion in Ch 2.
38 If a person is dissatisfied with the Privacy Committee's response, however, they are referred to the South Australian Ombudsman: see discussion in Ch 2.
39 The Tasmanian Ombudsman regulates privacy in Tasmania. The Northern Territory Information Commissioner is also responsible for overseeing freedom of information and the regulation of public records in the Northern Territory: see discussion in Ch 2.

Remedies

14.22 The remedies available to individuals whose privacy rights are infringed can differ according to the jurisdiction in which the complaint is made. For example, the maximum amount of compensation that is payable for an interference with privacy differs across the states and territories. The *Privacy Act* does not specify a limit on the payment of compensation. In contrast, the New South Wales Administrative Decisions Tribunal can order the payment of compensation of up to $40,000,[40] the Victorian Civil and Administrative Tribunal can order compensation of up to $100,000[41] and the Northern Territory Information Commissioner can order compensation up to $60,000.[42] There is no specific provision for compensation under the *Personal Information Protection Act 2004* (Tas). The Tasmanian Ombudsman, however, can make any order that he or she considers appropriate on finding a contravention of a Personal Information Protection Principle.[43] There is no provision for compensation under the Queensland privacy scheme.

14.23 In Chapter 46, the ALRC examines various issues related to the enforcement of the *Privacy Act*, including the payment of compensation and whether certain interferences with privacy should attract a civil penalty. To ensure a level of consistency in the outcome of privacy regulation, the states and territories should consider the range of enforcement tools, and the level of penalties and compensation, available under the *Privacy Act* and other state and territory privacy laws when developing privacy legislation.

State and territory legislation adopting *Privacy Act* provisions

14.24 Some state and territory legislation adopts federal legislation as a law of that state or territory in order to achieve national uniformity. This state and territory legislation usually includes a provision that indicates that the *Privacy Act* applies in relation to the adopted federal legislation. For example, competition policy reform legislation in each state and territory provides that the 'Commonwealth administrative laws' (defined to include the *Privacy Act*) apply in that jurisdiction to any matter arising in relation to the *Competition Code* of that jurisdiction.[44]

14.25 Other state and territory legislation applies specific provisions of the *Privacy Act*. For example, the *Road Transport (Vehicle Registration) Regulation 1998* (NSW) requires that the New South Wales Roads and Traffic Authority must treat a request for information about the particulars of a registrable vehicle in accordance with the IPPs.[45]

---

40 *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2)(a).
41 *Information Privacy Act 2000* (Vic) s 43.
42 *Information Act 2002* (NT) s 115.
43 *Personal Information Protection Act 2004* (Tas) s 22.
44 See, eg, *Competition Policy Reform (New South Wales) Act 1995* (NSW) s 30; *Competition Policy Reform (Tasmania) Act 1996* (Tas) s 30. See also, eg, *Agricultural and Veterinary Chemicals Act 1994* (Qld) s 16; *Water Efficiency Labelling and Standards Act 2005* (NSW) s 14.
45 *Road Transport (Vehicle Registration) Regulation 1998* (NSW) reg 15(7).

Stakeholders making submissions to this Inquiry did not identify any problems related to the adoption of *Privacy Act* provisions in state and territory laws.

Privacy rules, codes and guidelines

14.26 Various privacy rules, codes and guidelines regulate the handling of personal information, in addition to the *Privacy Act* and state and territory legislation.[46]

14.27 Part IIIAA of the *Privacy Act* allows private sector organisations and industries to develop and enforce their own privacy codes. Once a privacy code has been approved by the Privacy Commissioner, it replaces the NPPs for those organisations bound by the code. The *Privacy Act* requires that these codes contain standards equivalent to those in the NPPs, which would otherwise apply, or to a standard that secures individuals' privacy rights to a higher standard.[47]

14.28 A number of approved privacy codes provide higher standards than those provided in the NPPs. For example, the *Biometrics Institute Privacy Code* provides a number of 'Supplementary Biometrics Institute Privacy Principles' relating to protection, control and accountability.[48] There is no overlap with the NPPs, as a code replaces the NPPs for those organisations bound by it. However, an organisation may still be subject to other privacy regulation that is inconsistent with these codes. For example, an organisation that provides health services may engage in activities other than those dealt with under the *Biometrics Institute Privacy Code*, and is subject to the *Privacy Act* or a state or territory privacy regime in relation to these activities.

14.29 Federal legislation other than the *Privacy Act* also requires the development of privacy guidelines or codes. For example, under s 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth), the Minister may give the Director-General written guidelines to be observed by the Australian Security Intelligence Organisation (ASIO). The Attorney-General has issued two sets of guidelines concerning ASIO's functions—one in relation to obtaining intelligence relevant to security,[49] and another in relation to politically motivated violence.[50] The former contains guidelines on the treatment of personal information.[51] These guidelines are discussed further in Chapter 31.

---

46 See Ch 2.

47 *Privacy Act 1988* (Cth) s 16A.

48 Biometrics Institute, *Biometrics Institute Privacy Code—Public Register* (2006) <www.biometricsinstitute.org> at 3 August 2007, 16–18.

49 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of its Function of Obtaining Intelligence Relevant to Security* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007.

50 The guidelines in relation to politically motivated violence require that 'the collection of information concerning politically motivated violence be conducted with as little intrusion into privacy as is possible, consistent with the national interest': Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007, Guideline 3.2.

51 Ibid.

14.30 Some state regulatory regimes have adopted provisions from the *Privacy Act*. For example, the Victorian Essential Services Commission has developed *Guideline No 10 (Confidentiality and Informed Consent: Electricity and Gas)* (*Guideline No 10*). *Guideline No 10* requires Victorian electricity and gas retailers to comply with the NPPs whether or not they are 'organisations' under the *Privacy Act* and irrespective of when the personal information was collected. *Guideline No 10* also protects 'corporate customer information' as personal information. The Law Council of Australia has noted that this is a 'curious provision', given that the High Court of Australia has decided that corporations do not have a right to privacy at common law and that the *Privacy Act* protects the rights of individuals, not corporations.[52]

14.31 The Law Council has also noted that *Guideline No 10* requires retailers to apply the NPPs in a narrow way. For example, even if a retailer is providing the same customer with gas and electricity, *Guideline No 10* requires the retailer to handle separately customer information about the supply of each service. The Law Council argues that this is a much higher standard than the reasonable expectation test under NPP 2.1(a), and illustrates how the incorporation of NPP-like requirements into state legal regimes can lead to divergence over time.

14.32 Industry organisations have also developed guidelines. Some of these guidelines are not required by legislation. The Australian Direct Marketing Association (ADMA) has developed a *Direct Marketing Code of Practice* that binds ADMA members and all employees, agents, subcontractors and suppliers of ADMA members.[53] The Code includes a schedule that outlines principles to govern fair conduct relevant to consumer data protection.[54] The principles are based on the NPPs and deal with such matters as: limitations on the amount of information that companies can collect about individuals; informing consumers about who is collecting information, and how the company can be contacted; and the intended use of the personal information. Consumers must be given the opportunity to opt out of future direct marketing approaches and block transfer of their contact details to any other marketer.

Submissions and consultations

14.33 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether privacy rules, codes and guidelines developed under federal, state and territory legislation, or by organisations and industry groups, contribute to fragmentation and inconsistency in the regulation of personal information.[55]

---

52 Law Council of Australia, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act*, 22 December 2004.

53 Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2001), [6]. For further discussion of the Code see Ch 1.

54 Ibid, sch E.

55 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–9.

14.34 A number of submissions noted that if rules, codes and guidelines are not aligned with the *Privacy Act*, they can contribute to inconsistency and fragmentation.[56] The Office of the Victorian Privacy Commissioner noted that codes, rules and guidelines can offer less protection than is available under privacy laws where they do not offer individuals a right of complaint or the ability to seek redress for harm suffered.[57] The Australian Retailers Association submitted that a central resource of information on regulatory instruments, including industry codes of practice, should be established and maintained by the OPC.[58]

14.35 Stakeholders also noted, however, that while it is important to limit unnecessary fragmentation of privacy law, additional privacy rules, codes and guidelines can clarify sector-specific issues and provide more detailed protection for personal information where appropriate.[59] The Australian Privacy Foundation submitted that the wide range of privacy rules, codes and guidelines contribute to fragmentation and inconsistency in the regulation of personal information, but noted that with a unified set of privacy principles and greater national consistency there would still be a valuable role for sector or activity specific guidelines and codes.[60]

ALRC's view

14.36 The ALRC acknowledges that privacy rules, codes and guidelines can be beneficial where there is a need for privacy rules to be crafted to the specific needs and practices of particular organisations or industry groups. These documents can, however, contribute to fragmentation and inconsistency of privacy regulation when they are not aligned with existing privacy laws.

14.37 In the ALRC's view, when agencies and organisations are developing privacy rules, codes and guidelines they should consult with the relevant body responsible for privacy for their industry or sector to ensure that the rules, codes or guidelines will interact and operate effectively with existing privacy laws. Further, agencies and organisations should ensure that the privacy rules, codes and guidelines outline who an individual can approach with a privacy issue or complaint.

Residential tenancy databases

14.38 Residential tenancy databases (RTDs) raise a range of issues. They are dealt with here because they are currently regulated by inconsistent and fragmented federal,

---

56 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; CSIRO, *Submission PR 176,* 6 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007.

57 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

58 Australian Retailers Association, *Submission PR 131,* 18 January 2007.

59 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

60 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

state and territory legislation. A number of inquiries have identified the need for national consistency in the regulation of RTDs.

14.39 RTDs are electronic databases operated by private companies that contain information about tenants and their rental history. The purpose of such databases is to enable real estate agents to assess 'business risk' on behalf of the property owner. The listings on the database are based on information provided by real estate agents to the database operators. Listings are generally collected from across Australia and can be accessed nationally.

14.40 A number of issues have been raised in relation to RTDs. For example, recent inquiries have heard that prospective tenants will often have little choice but to consent to a real estate agent passing information on to RTD operators,[61] that information stored on RTDs is sometimes inaccurate,[62] and that tenants sometimes have difficulties in finding out whether they are listed on RTDs.[63]

14.41 In April 2004, the Privacy Commissioner made four determinations concerning a residential tenancy database operator. These determinations included that the operator had breached a number of the NPPs by:

- using an agreement with its members that did not specify sufficiently the data quality standards required;
- failing to take sufficient steps to check listings by property managers and not requiring minimum identification requirement before listing;
- failing to advise tenants contemporaneously that they had been listed;
- using a 'pick list' method of reporting tenancy history, which relied on one category that was broadly defined and on descriptions that were brief, not consistently defined and not mutually exclusive;
- providing an inadequate dispute resolution process;
- failing to provide mechanisms to correct records where the individual concerned had established they were not accurate, complete and up-to-date or to associate a statement to this effect when there was a dispute about accuracy, completeness or currency;
- charging individuals an excessive amount of money for access via mail to their personal information;

---

61 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 87.

62 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), [3.4.8].

63 Victorian Law Reform Commission, *Residential Tenancy Databases* (2006).

- failing to take reasonable steps to make sure the personal information it collected, used and disclosed was up-to-date; and
- failing to take reasonable steps to destroy or de-identify personal information that was no longer needed for any purpose.[64]

14.42 RTDs contain personal information and so are generally subject to the private sector provisions of the *Privacy Act*. They are also regulated by legislation in some states and territories. The *Privacy Act* applies to RTD operators with an annual turnover of $3 million or less, despite the small business exemption, because they trade in personal information.[65] If an RTD operator that is a small business gains consent for the collection or disclosure of an individual's personal information, however, the *Privacy Act* will not apply.[66] Further, the *Privacy Act* does not contain provisions directed specifically at RTD operators. For example, unlike credit reporting agencies, there is no provision under the *Privacy Act* relating to time limits for the removal of default listings.[67]

14.43 While the states and territories can regulate the actions of the lessors and agents in their jurisdictions, they lack the power to regulate effectively RTD operators based in different jurisdictions.[68] Residential tenancy legislation in New South Wales, Queensland, and now the ACT regulates how real estate agents and lessors list tenants on RTDs.[69] This legislation, however, is incomplete and inconsistent. For example, while the *Property Stock and Business Agents Regulation 2003* (NSW) provides for the length of time information can be listed[70] and whether a listed person can access the listing information,[71] the *Residential Tenancies Act 1994* (Qld) does not. In South Australia and the Northern Territory some regulation is provided through fair trading legislation.[72] This is primarily consumer protection legislation, however, and does not specifically relate to RTDs.

14.44 A number of inquiries have now recognised the need for national consistency in the regulation of RTDs.[73] In August 2003, the Ministerial Council on Consumer

---

64 Office of the Federal Privacy Commissioner, *Complaint Determination No 1 of 2004*, 1 April 2004; Office of the Privacy Commissioner, *Complaint Determination No 2 of 2004*, April 2004; Office of the Privacy Commissioner, *Complaint Determination No 3 of 2004*, April 2004; Office of the Privacy Commissioner, *Complaint Determination No 2 of 2004*, April 2004.

65 See *Privacy Act 1988* (Cth) s 6D(4)(c)–(d); Office of the Privacy Commissioner, *Complaint Determination No 3 of 2004*, April 2004.

66 *Privacy Act 1988* (Cth) s 6D(7), (8).

67 Ibid s 18F.

68 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), [3.2].

69 *Property Stock and Business Agents Regulation 2003* (NSW); *Residential Tenancies Act 1994* (Qld); *Residential Tenancies Act 1997* (ACT).

70 *Property Stock and Business Agents Regulation 2003* (NSW) sch 6A, cl 6(c).

71 Ibid sch 6A, cl 64(a).

72 See, eg, *Fair Trading Act 1987* (SA) pt 4; *Consumer Affairs and Fair Trading Act 2004* (NT) pt 8.

73 Victorian Law Reform Commission, *Residential Tenancy Databases* (2006), [6.5] and rec 1; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 72–73; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Ministerial Council on

Affairs (MCCA) agreed with the Standing Committee of Attorneys-General (SCAG) to establish a joint Residential Tenancy Database Working Party. The Working Party released its *Report on Residential Tenancy Databases* on 27 September 2005. The Working Party found that ensuring national uniformity in the treatment of RTDs was essential. It stated, however, that it was inappropriate for the Australian Government to legislate for RTDs and their use by agents, given the existing state and territory responsibilities for agents and tenancy issues.[74]

14.45 The Working Party expressed the view that state and territory legislation should address the relationship between the agent and the tenant, including issues such as informing the tenant about the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs. The Working Party recommended that the states and territories develop agreed uniform model legislation on the use of RTDs by landlords, agents and listing parties. In April 2006, SCAG agreed to the development of model uniform legislation for RTDs. The MCCA has primary responsibility for drafting the legislation.

14.46 The Working Party also concluded that, because the states and territories would generally not be able to regulate directly the operation of the RTDs or their interaction with agents, the *Privacy Act* should regulate this aspect of the operation of RTDs. The Working Party was concerned, however, that, because of the small business exemption, a tenant's consent to the collection or disclosure of their personal information also removes other privacy obligations from the RTD operator, such as those in relation to data quality. The Working Party recommended, therefore, that regulations should be made pursuant to s 6E of the *Privacy Act* to prescribe all RTDs as organisations for the purposes of the *Privacy Act*.

14.47 The Working Party also noted that the *Privacy Act* is not prescriptive and does not permit the OPC to direct RTD operators to comply with their obligations under the Act. The Working Party therefore recommended that the Australian Government consider the option of a binding code if RTD operators do not comply with the *Privacy Act*.[75]

Submissions and consultations

14.48 In IP 31, the ALRC asked how personal information held on residential tenancy databases should be regulated. The ALRC also asked whether residential tenancy

---

Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

74 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

75 As recommended by the Privacy Commissioner in Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 16. Binding codes are considered in Ch 44.

databases should be regulated under the *Privacy Act*, by a binding code, or in some other way.[76]

Are RTDs necessary?

14.49 The Real Estate Institute of Australia and the Institute of Mercantile Agents submitted that RTDs are an effective risk management tool. It was said that while the cost of access is minimal, failure to do so can be expensive in terms of potential litigation, professional negligence, property damage and loss of rent. The Real Estate Institute of Australia noted that a RTD listing should never be used in a threatening manner to ensure the performance of a tenant.[77]

14.50 The Tenants Union of Victoria submitted, however, that whether RTDs are an appropriate means of managing risk is contentious because of the potential for listing to restrict opportunities in the private rental market. It noted that damage or financial loss arising from leasing out residential property is a foreseeable business risk that should be ameliorated with insurance, because the consequences of restricted access to housing have a detrimental impact on both individual tenants and the community at large.[78]

Concerns about RTDs

14.51 A number of submissions raised concerns about the operation of RTDs. Some submissions noted that tenants are often given little choice when signing tenancy agreements and RTD users routinely extract 'consent' from tenancy applicants. Submissions also noted that information held on RTDs is sometimes inaccurate.[79] It was also noted that many tenants are unaware that they are listed on an RTD, and that some tenants may not discover they have been listed until months or sometimes years later.[80]

14.52 Stakeholders observed that RTDs can make it difficult for Australian households reliant on the private rental market to secure housing.[81] Anglicare Tasmania submitted that, with the chronic shortage of medium-term crisis accommodation and the long waiting lists for public housing, private rental housing is often the only option for vulnerable and low income households.[82]

---

76 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–3.

77 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

78 Tenants Union of Victoria Ltd, *Submission PR 197,* 16 February 2007.

79 Tenants Union of NSW Co-op Ltd, *Submission PR 169,* 5 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

80 Tenants Union of Victoria Ltd, *Submission PR 197,* 16 February 2007.

81 Ibid.

82 Anglicare Tasmania, *Submission PR 135,* 19 January 2007.

14.53 The ALRC heard that inconsistent state legislation in relation to RTDs causes a number of problems.[83] It was submitted, for example, that inconsistent state and territory laws have resulted in varying listing practices across Australia and that this can result in people being listed on an RTD for life.[84] It was also observed that state legislation does not directly regulate RTDs,[85] and that in some jurisdictions there is no body to complain to about RTD matters.[86]

How should RTDs be regulated?

14.54 A number of submissions endorsed uniform state and territory legislation to regulate the use of RTDs by landlords, agents and other listing parties.[87] Other submissions argued that all RTD operators should be brought under the *Privacy Act* and that the OPC should make a binding code in relation to them.[88] A number of submissions supported both state and territory legislation and a binding code under the *Privacy Act*.[89]

14.55 The OPC submitted that if the states and territories do not pass uniform legislation, the *Privacy Act* should be amended to define all RTD operators as 'organisations' for the purposes of the *Privacy Act*. The OPC submitted that a binding code in relation to RTDs may be appropriate, noting that the NPPs may not be specific enough to address particular concerns about RTDs, such as data retention periods.[90] The Tenants Union of NSW was concerned that a binding code under the *Privacy Act* may not make provision for dispute resolution by state and territory tenancy tribunals.

> These forums are relatively accessible, quick, affordable and experienced in housing matters, and could deal with RTD disputes and other disputes arising from a tenancy in the same proceedings. Whether RTD regulation is pursued through nationally uniform legislation by each State and Territory, or through a binding code under the *Privacy Act 1988*, we submit that it should provide dispute resolution through the State and Territory Tenancy Tribunals.[91]

---

83 Tenants Union of Victoria Ltd, *Submission PR 197,* 16 February 2007; Anglicare Tasmania, *Submission PR 135,* 19 January 2007. See also R Harrison and D Imber, 'Residential Tenancy Databases: Need for National Regulation' (2007) 3(8) *Privacy Law Bulletin* 98.

84 Tenants Union of Victoria Ltd, *Submission PR 197,* 16 February 2007.

85 Tenants Union of NSW Co-op Ltd, *Submission PR 169,* 5 February 2007.

86 Anglicare Tasmania, *Submission PR 135,* 19 January 2007.

87 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

88 Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Anglicare Tasmania, *Submission PR 135,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

89 See, eg, Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Tenants Union of NSW Co-op Ltd, *Submission PR 169,* 5 February 2007.

90 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

91 Tenants Union of NSW Co-op Ltd, *Submission PR 169,* 5 February 2007.

14.56 The Real Estate Institute of Australia supported the establishment of state and territory legislation to deal with the tenant and agent relationship in relation to RTD, and bringing all RTD operators under the *Privacy Act*. The Institute did not, however, believe that the need for a binding code on RTD operators had yet been demonstrated, but may be supportive in the future if this is required.[92]

What rules should apply to the use and operation of RTDs?

14.57 Stakeholders noted that laws regulating the use and operation of RTDs should address a number of issues. It was submitted that these laws should include:

- requirements on users of RTDs to inform applicants that they use RTDs, that they have been listed on a RTD, how to contact the RTDs they use, and how to dispute a listing;
- an obligation on any user of a RTD to inform that tenant of the content of any listing found;
- a set of criteria that determines when a listing can be made;
- a requirement to give a tenant an opportunity to respond to or dispute a listing;
- a requirement that a listing specify the ground for the listing and, where the ground is that the person owes money, specify the amount of the debt;
- a provision noting a time period after the end of a tenancy after which a person may not be listed on a RTD;.
- a protocol for the removal of listings once the issue that initiates the listing has been resolved; and
- the expiration of a listing after a reasonable period of time.[93]

ALRC's view

14.58 A number of reviews have established the need for stronger and nationally consistent regulation of RTDs. The ALRC shares the concerns raised in these reviews and of those who made submissions to this Inquiry in relation to the collection, use and disclosure of personal information held on RTDs. The ALRC affirms the recommendations of the RTD Working Party that the states and territories should enact legislation that addresses the relationship between the agent and the tenant, including issues such as: informing the tenant about the use of RTDs and the collection of information; and the way that agents interact with RTDs, including such matters as controlling the information provided by agents to RTDs.

14.59 Further, the ALRC considers that all RTD operators should be regulated by the *Privacy Act*, irrespective of whether they are small business operators or whether they

---

92 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

93 Tenants Union of Victoria Ltd, *Submission PR 197,* 16 February 2007; Tenants Union of NSW Co-op Ltd, *Submission PR 169,* 5 February 2007; Anglicare Tasmania, *Submission PR 135,* 19 January 2007.

gain consent for the collection or disclosure of an individual's personal information. In Chapter 35, the ALRC proposes the removal of the exemption that applies to small businesses under the *Privacy Act*. The removal of this exemption should deal with this issue. If, however, the small business exemption is not removed, it is the ALRC's view that regulations should be made pursuant to s 6E of the *Privacy Act* to prescribe all RTDs as organisations for the purposes of the Act.

14.60 The ALRC notes that on 13 August 2007, the Attorney-General of Australia announced that regulations to extend the coverage of the *Privacy Act* to all RTDs were complete. The regulations will commence on 1 December 2007 to allow small business operators of RTDs sufficient time to comply with the requirements of the *Privacy Act*.[94]

14.61 The ALRC does not at this time propose the making of a binding code to regulate RTD operators. It is the ALRC's view that state and territory legislation regulating the use of RTDs and the regulation of RTD operators by the *Privacy Act* should deal with many of the issues identified in submissions. The ALRC has, however, proposed that the *Privacy Act* should be amended to empower the Privacy Commissioner to develop and impose a privacy code that applies to designated agencies and organisations (a 'binding code').[95] Following the implementation of this proposal, the OPC should monitor the use and operation of RTDs in order to determine whether it should exercise its powers to impose a binding code on RTD operators. The OPC could also request that RTD operators develop a privacy code to be approved by the Privacy Commissioner.[96]

14.62 The ALRC notes stakeholders' concerns that tenants with privacy complaints about the handling of personal information by RTD operators should be able to have those complaints dealt with by a state or territory tenancy tribunal or an equivalent body. These bodies are well suited to deal with privacy matters in the residential tenancy context—they are quick, accessible and affordable. In Chapter 45, the ALRC proposes that the *Privacy Act* be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of his or her powers in relation to complaint handling. In the ALRC's view, it would be appropriate for the Privacy Commissioner to delegate his or her complaint-handling powers in relation to RTD operators to state and territory tenancy tribunals and equivalent bodies under this section.

---

94 P Ruddock (Attorney-General), 'Privacy for Residential Tenants' (Press Release, 13 August 2007).
95 See Ch 44.
96 See Ch 44.

Australian Government
Australian Law Reform Commission

Review of Australian Privacy Law

DISCUSSION PAPER

You are invited to provide a submission or comment on this Discussion Paper

VOLUME 2
DISCUSSION PAPER 72
SEPTEMBER 2007

This Discussion Paper reflects the law as at 31 July 2007

ISBN- 978-0-9758213-9-8

Commission Reference: DP 72

The Australian Law Reform Commission was established on 1 January 1975 by the *Law Reform Commission Act 1973* (Cth) and reconstituted by the *Australian Law Reform Commission Act 1996* (Cth). The office of the ALRC is at Level 25, 135 King Street, Sydney, NSW, 2000, Australia.

All ALRC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the ALRC.

Telephone:	within Australia	(02)	8238 6333
	International	+61 2	8238 6333
TTY:		(02)	8238 6379
Facsimile:	within Australia	(02)	8238 6363
	International	+61 2	8238 6363

E-mail: info@alrc.gov.au

ALRC homepage: www.alrc.gov.au

Printed by Ligare Pty Ltd

Summary of Contents

Volume 1

Part A – Introduction 101

1. Introduction to the Inquiry 103
2. Overview—Privacy Regulation in Australia 145
3. The *Privacy Act* 169
4. Achieving National Consistency 235
5. Protection of a Right to Personal Privacy 277

Part B – Developing Technology 309

6. Overview—Impact of Developing Technology on Privacy 311
7. Accommodating Developing Technology in a Regulatory Framework 341
8. Individuals, the Internet and Generally Available Publications 375
9. Identity Theft 393

Part C – Interaction, Inconsistency and Fragmentation 404

10. Overview—Interaction, Inconsistency and Fragmentation 405
11. The Costs of Inconsistency and Fragmentation 419
12. Federal Information Laws 447
13. Required or Authorised by or under Law 487
14. Interaction with State and Territory Laws 519

Volume 2

Part D – The Privacy Principles 541

15. Structural Reform of Privacy Principles 543
16. Consent 571

17. Anonymity and Pseudonomity **587**
18. Collection **599**
19. Sensitive Information **613**
20. Specific Notification **627**
21. Openness **651**
22. Use and Disclosure **667**
23. Direct Marketing **699**
24. Data Quality **719**
25. Data Security **729**
26. Access and Correction **755**
27. Identifiers **775**
28 Transborder Data Flows **815**
29. Additional Privacy Principles **865**

Part E – Exemptions 875

30. Overview—Exemptions from the *Privacy Act* **877**
31. Defence and Intelligence Agencies **899**
32. Federal Courts and Tribunals **927**
33. Exempt Agencies under the *Freedom of Information Act 1982* (Cth) **955**
34. Other Public Sector Exemptions **975**
35. Small Business Exemption **1007**
36. Employee Records Exemption **1039**
37. Political Exemption **1065**
38. Media Exemption **1081**
39. Other Private Sector Exemptions **1113**
40. New Exemptions **1123**

Part F – Office of the Privacy Commissioner 1141

41. Overview—Office of the Privacy Commissioner **1143**
42. Facilitating compliance with the *Privacy Act* **1151**
43. Structure of the Office of the Privacy Commissioner **1159**

44. Powers of the Office of the Privacy Commissioner 1185
45. Investigation and Resolution of Privacy Complaints 1239
46. Enforcing the *Privacy Act* 1275
47. Data Breach Notification 1293

Volume 3

Part G – Credit Reporting Provisions 1321
48. Overview—Credit Reporting 1323
49. The Credit Reporting Provisions 1337
50. The Approach to Reform 1359
51. More Comprehensive Credit Reporting 1401
52. Collection of Credit Reporting Information 1445
53. Use and Disclosure of Credit Reporting Information 1475
54. Data Quality and Security 1503
55. Rights of Access, Complaint Handling and Penalties 1529

Part H – Health Services and Research 1557
56. Regulatory Framework for Health Information 1559
57. The Privacy Act and Health Information 1595
58. Research 1653

Part I – Children, Young People and Adults Requiring Assistance 1713
59. Children, Young People and Privacy 1715
60. Decision Making by Individuals Under the Age of 18 1751
61. Adults with a Temporary or Permanent Incapacity 1815
62. Other Third Party Assistance 1839

Part J – Telecommunications **1847**

63. *Telecommunications Act* **1849**

64. Other Telecommunications Privacy Issues **1901**

Part D

The Privacy Principles

15. Structural Reform of the Privacy Principles

Contents

Introduction to Part D 543
Development of current Australian privacy principles 544
OECD Guidelines 544
Information Privacy Principles 547
National Privacy Principles 547
Principles-based regulation of privacy 548
The differing types of regulation 548
What is principles-based regulation? 550
Choice of regulatory mechanism: principles or rules? 550
Level of detail, guidance and protection 554
Background 554
Submissions and consultations 555
ALRC's view 558
Towards a single set of privacy principles 560
Background 560
Previous privacy inquiries 562
Submissions and consultations 563
ALRC's view 566
Scope and structure of Unified Privacy Principles 567
Scope of Unified Privacy Principles 567
Structure of a single set of privacy principles 567
ALRC's view 569

Introduction to Part D

15.1 Part D of this Discussion Paper proposes reform to the privacy principles in the *Privacy Act 1988* (Cth). Currently, the Act contains two sets of privacy principles: the Information Privacy Principles (IPPs),[1] which apply predominantly to public sector 'agencies'; and the National Privacy Principles (NPPs),[2] which apply to private sector 'organisations'.[3] Both sets of privacy principles are directed only to personal

1 See *Privacy Act 1988* (Cth) s 14.
2 See Ibid sch 3.
3 The terms 'agency' and 'organisation' are defined, respectively, in Ibid ss 6(1) and 6C.

information. That is, they do not cover other areas of privacy such as bodily privacy, privacy from surveillance, or communications privacy.

15.2 In this Part, the ALRC proposes to reform the existing privacy principles in two ways: first, by consolidating the IPPs and NPPs; and secondly, by amending, where warranted, the substantive content of the privacy principles. This chapter concentrates on how the structure of the privacy principles should be reformed. It explains how the IPPs and NPPs currently operate. The chapter then presents the ALRC's views on how to bring together the NPPs and IPPs, by creating a single, unified set of privacy principles (the Unified Privacy Principles or UPPs), which will be of general application across the public and private sectors. The name used in this Discussion Paper to designate the consolidated privacy principles—the Unified Privacy Principles—is designed to reflect the fact that they are the product of unifying the IPPs and NPPs. It should be noted that, in the event that the ALRC's relevant proposals are adopted, it may be more appropriate to use a different term to describe the privacy principles in the Act.

15.3 The remaining chapters in Part D propose reform to the substantive content of the privacy principles in the *Privacy Act*. This analysis is made largely on the assumption that the ALRC's proposals in this chapter are adopted. Even if some or all of the proposals in this chapter are not adopted, however, the proposals in this Part remain applicable insofar as they suggest amendments that respond to problems identified in the Act's two sets of privacy principles, the IPPs and NPPs.

15.4 The ALRC analyses the privacy principles thematically. In relation to each theme of privacy, there is a brief explanation of how the IPPs and NPPs currently apply and a summary of any relevant issues relating to their operation. This is followed by the ALRC's proposals for how to reform the privacy principle in question. Finally, this chapter contains a summary of how the ALRC envisages the Unified Privacy Principles will appear, if the ALRC's proposals are adopted.

Development of current Australian privacy principles

OECD Guidelines

15.5 The preamble to the *Privacy Act* notes that Australia is a member of the Organisation for Economic Co-operation and Development (OECD); that the Council of the OECD has recommended that member countries take into account in their domestic legislation the privacy principles set out in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines); and that Australia has expressed its intention to participate in the recommendation. The privacy principles in the OECD Guidelines are the foundation for the two sets of privacy principles in the *Privacy Act*: the IPPs and the NPPs.

15.6 The OECD Guidelines were designed to discourage the member countries of the OECD from introducing 'incompatible and conflicting laws for the defence of privacy

in the newly established databases of the interlinked information technologies'.[4] As such, the OECD Guidelines have influenced data protection laws in many jurisdictions.

15.7 The OECD Guidelines attempt to reconcile sometimes competing interests—that is, the goal of protecting privacy and individual liberties is balanced with the desire to advance the free flow of personal data.[5] The Guidelines were developed to harmonise national privacy legislation and, while upholding human rights, simultaneously to prevent interruptions in international flow of data.[6]

15.8 The OECD Guidelines apply to 'personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties'.[7] On one hand, they are 'minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties'.[8] On the other hand, the Guidelines deter member countries from creating unnecessary obstacles to transborder flows of personal data in the name of the protection of privacy and individual liberties.[9]

15.9 Part Two of the OECD Guidelines sets out eight basic principles of national application: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.[10] These principles are covered explicitly in the IPPs, NPPs and proposed UPPs. Although there is no principle called 'Accountability', aspects of this principle are incorporated in other provisions in the Act, such as those dealing with investigations of complaints regarding privacy breaches.[11]

15.10 A critical question faced both by the drafters of the OECD Guidelines and member states seeking to implement the Guidelines is: what should be articulated in general privacy principles and what should be the content of detailed machinery provisions? The Explanatory Memorandum to the OECD Guidelines states:

> The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions … should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same

---

4 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 25.

5 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [25].

6 Ibid, preface.

7 Ibid, Guideline 2.

8 Ibid, Guideline 6.

9 Ibid, Guideline 18.

10 See Ibid, Guidelines 7–14.

11 See Part F of this Discussion Paper, which discusses the data breach issue and the powers of the Office of the Privacy Commissioner.

> applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a dividing line between the level of basic principles or objectives and lower level 'machinery' questions which should be left to domestic implementation.[12]

15.11 John Gaudin has expressed the view that the OECD Guidelines are grounded in the society, technology and culture of the 1970s and that the principles are insufficiently flexible to accommodate the extensive changes that have taken place since they were promulgated.[13] He has stated that the OECD Guidelines reflect assumptions about the future development of information technology, which are now seen to be limited.[14] Justice Michael Kirby, who chaired the OECD Expert Group on Privacy, has stated extra-judicially:

> There appears to be a need to review the 1980 OECD Guidelines, which are already showing signs of their age. Informed writers are already suggesting the necessity for privacy principles apt to contemporary technology. … Clearly the 'openness principle' of the OECD Guidelines was always one of the weakest. The advent and potential of the internet require that there be new attention to it.[15]

15.12 In addition to the OECD Guidelines, on 26 November 1992, the Council of the OECD adopted the *Guidelines for the Security of Information Systems*. These further Guidelines aimed 'to raise awareness of risks to information systems and of the safeguards available to meet those risks', and 'to create a framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems'.[16] Due to the dramatic change in the information technology environment since 1992, those Guidelines were replaced by the OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, which were adopted on 25 July 2002 (the OECD Security Guidelines).

15.13 The OECD Security Guidelines contain nine information systems security principles: awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment. For example, the awareness principle provides that 'participants should be aware of the need for security of information systems and networks and what they can do to

---

12 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19 (e)]. See also [50].

13 J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part II' (1997) 3 *Privacy Law & Policy Reporter* 196, 199.

14 See J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part I' (1996) 3 *Privacy Law & Policy Reporter* 143, 144.

15 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 27. The question whether the *Privacy Act* should be technologically neutral is addressed in Ch 7.

16 See Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems* (1992).

enhance security'[17] and the response principle provides that 'participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents'.[18]

Information Privacy Principles

15.14 Section 14 of the *Privacy Act* contains the 11 Information Privacy Principles or IPPs. The IPPs were included in 1988 in the original version of Act, and they have not been amended since that time. Until 2000, the IPPs were the only privacy principles in the Act.

15.15 The IPPs regulate the collection, storage, use and disclosure of an individual's personal information, and provide for individuals to access and correct their personal information. As noted above, the IPPs apply to personal information handled by Commonwealth and ACT government agencies.[19]

15.16 The Privacy Commissioner has issued a series of guidelines on the interpretation of the principles.[20] The guidelines note that:

> The IPPs set out minimum standards for agencies. Compliance with the IPPs is a legal obligation, but minimal compliance will not always be an appropriate approach for an agency to take. … Especially where sensitive information is concerned, or where mishandling of personal information may have serious consequences, more care to protect individuals' privacy may be appropriate than is required by the letter of the IPPs.[21]

National Privacy Principles

15.17 Schedule 3 to the *Privacy Act* contains 10 further privacy principles, the National Privacy Principles or NPPs. Schedule 3 was not part of the original Act; instead, it was introduced by the *Privacy Amendment (Private Sector) Act 2000* (Cth).

---

17 Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002), Principle 1.

18 Ibid, Principle 3.

19 See *Privacy Act 1988* (Cth) ss 13(a), 16. The definition of 'agency' in *Privacy Act 1988* (Cth) s 6(1) includes: a Minister; a Department; a body established for a public purpose; a federal court; and the Australian Federal Police. This definition is discussed in greater detail in Ch 3.

20 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994); Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998); Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996). The status of guidelines is discussed in Part F of this Discussion Paper.

21 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998).

15.18 The NPPs apply generally to private sector 'organisations', unless the organisation in question is subject to an approved privacy code.[22] The term 'organisation' is defined in s 6C as an individual, a body corporate, a partnership, any other unincorporated association or a trust. However, this definition is subject to a number of qualifications, exempting, among others, small business operators, political parties, government agencies, and state or territory authorities and prescribed instrumentalities.[23]

15.19 The NPPs regulate the following aspects of how personal information should be managed: how data are collected; how data are used and disclosed; data quality; data security; openness of data management policies; individuals' rights of access and correction; the use of identifiers; individuals' right to maintain their anonymity; transborder data flows; and how sensitive information should be treated.

15.20 The stated objectives of the NPP regime are:

> (a) to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations; and
>
> (b) to do so in a way that:
>
> (i) meets international concerns and Australia's international obligations relating to privacy; and
>
> (ii) recognises individuals' interests in protecting their privacy; and
>
> (iii) recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently.[24]

Principles-based regulation of privacy

The differing types of regulation

15.21 The NPPs and IPPs—together referred to as the privacy principles—represent the main regulatory mechanism in the *Privacy Act*. Parliament deemed it preferable to regulate privacy using broad principles, as distinct from using a more conventional method of rules-based regulation. This part of the chapter is partly descriptive and partly analytical: it describes how principles-based regulation differs from rules-based regulation, and it analyses the strengths and limitations of each regulatory system.

---

22 *Privacy Act 1988* (Cth) s 16A. See also the relevant Second Reading Speech: Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15749–15750. Note that privacy codes are discussed in Part F of this Discussion Paper.

23 The definition of 'organisation' is discussed in greater detail in Ch 3. The private sector exemptions to the *Privacy Act* are discussed in Part E.

24 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3.

15.22 In order to understand what is principles-based regulation, it is necessary first to consider the differing ways in which government can regulate. Professor Julia Black posits the existence of three broad categories of regulatory method: 'bright line' rules; 'principles' and 'complex or detailed rules'.[25] Table 15.1 below provides hypothetical examples of each of these three types of regulatory method. The paragraphs immediately following it explain how these different forms of regulation operate.[26]

Table 15.1: Hypothetical examples of regulatory methods

Bright line rule	Principle	Complex/detailed rule
An organisation must not collect personal information relating to an individual's sexuality.	An organisation must not collect personal information unless it is necessary for one of its functions or activities.	An organisation [defined] must not collect [defined] personal information [defined] unless all of the following conditions are met: [list of conditions].

15.23 As Table 15.1 illustrates, a 'bright line' rule contains a single criterion of applicability. Such rules are clear and straightforward to apply but can fail to achieve their goal because there is considerable scope for manipulation or creative compliance. For instance, the rule may not be broad enough to capture all of the conduct that it is intended to proscribe, or an organisation may seek a loophole so as to comply with the letter, but not the spirit, of the rule.

15.24 A 'principle' articulates substantive objectives. Whether or not a principle is certain depends on whether there is general consensus about what is required to achieve compliance. While principles may appear simple to apply—in that they are concise and avoid arcane language—problems can arise in practice where, for instance, there is a dispute as to the meaning of the key terms. In the example from Table 15.1 above, reasonable minds may differ over what is necessary, in a particular context, for an organisation's functions or activities.

15.25 A complex or detailed rule can provide a higher degree of certainty because it expressly lists the relevant conditions to be taken into account. Applying such a rule is, however, complex and the creation of a list of conditions inevitably will leave gaps resulting in scope for manipulation or creative compliance.

---

25 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10. There are, of course, many other ways of differentiating between the various methods of regulation. See, eg, R Baldwin, *Rules and Government* (1995), 7–11.

26 This part of the chapter is adapted from J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10.

What is principles-based regulation?

15.26 According to Black, principles are 'general rules … [that] are implicitly higher in the implicit or explicit hierarchy of norms than more detailed rules: they express the fundamental obligations that all should observe.' Black states that principles-based regulation avoids 'reliance on detailed, prescriptive rules and rel[ies] more on high-level, broadly stated rules or principles'.[27]

15.27 Part of the guiding purpose of a principles-based approach is to shift the regulatory focus from *process* to *outcomes*. The rationale for this is described as follows:

> regulators, instead of focussing on prescribing the processes or actions that firms must take, should step back and define the outcomes that they require firms to achieve. Firms and their management will then be free to find the most efficient way of achieving the outcome required.[28]

15.28 Thus, principles-based regulation seeks to provide an overarching framework that guides and assists regulated entities to develop an appreciation of the core goals of the regulatory scheme. A key advantage of principles-based regulation is its facilitation of regulatory flexibility through the statement of general principles that can be applied to new and changing situations. It has been said that such a regulatory framework is exhortatory in that it emphasises a 'do the right thing' approach and promotes compliance with the spirit of the law.[29]

Choice of regulatory mechanism: principles or rules?

15.29 According to Black, all forms of regulation are subject, to varying degrees, to the following problems:

- *Rules are just a 'best guess' as to the future*: The rule maker has to anticipate how the rule will be applied in the future. New situations may arise that were not expected/known about when the rule was written, and the rule may be interpreted and applied in ways that were not intended or anticipated by the writer.
- *Rules are never perfectly congruent with their purpose …* : Rules are inevitably either under-inclusive, failing to catch things that the rule maker might want to catch, and/or over-inclusive, catching things that the rule maker might not want to catch when applied to particular sets of circumstances …
- *Whether a rule is clear or certain depends on shared understandings*: Just looking at a rule does not tell us whether it is certain. … Whether or not a rule is 'certain' depends not so much on whether it is detailed or general,

---

27 Ibid, 3.
28 Ibid, 5.
29 S Arjoon, 'Striking a Balance Between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68 *Journal of Business Ethics* 53, 69.

> but whether all those applying the rule (regulator, regulated firm, court/tribunal) agree on what the rule means.
>
> - *How a rule affects behaviour does not depend solely on the rule*: … whether a rule has the desired effect on behaviour depends only partly on whether it is a precise, detailed rule or whether it is a principle. The firm's own attitude to regulation, the incentive structures for compliance and non-compliance, and the approach taken to enforcement, are also critical.[30]

15.30 Principles-based regulation attempts to solve these problems, largely by providing greater 'flexibility', thereby allowing for 'a greater degree of "future-proofing", enabling the regime to respond to new issues as they arise without having to create new rules'.[31] Future-proofing can be achieved by drafting purposive principles that both express the rationale for the rule and provide 'overarching requirements that can be applied flexibly to a rapidly changing industry'. Principles-based regulation also makes use of qualitative and often evaluative terms such as fair, reasonable and suitable.[32] This regulatory approach can facilitate compliance as it allows entities to honour the spirit of the law by developing policies or other mechanisms that simultaneously comply with the rule and meet the entity's needs.

15.31 By contrast, rules-based regulation is comparatively rigid. Detailed rules impose requirements that are not always appropriate for all entities regulated by the relevant scheme and, further, they do not always cover all of the entities or activities that are intended to be regulated.[33] Black states:

> Detailed rules, it is often claimed, provide certainty, a clear standard of behaviour and are easier to apply consistently and without retrospectivity. However, they can lead to gaps, inconsistencies, rigidity and are prone to 'creative compliance', to the need for constant adjustment to new situations and to the ratchet syndrome, as more rules are created to address new problems or close new gaps, creating more gaps and so on.[34]

15.32 On the other hand, a regulatory approach that is based on using prescriptive rules can provide greater clarity in the regulation, as it is easier for a regulated entity to determine what rules it must comply with and the minimum standards of compliance

---

30 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 8.

31 Ibid, 7.

32 Ibid, 4.

33 O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 330–331.

34 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 7.

expected.[35] This can, in turn, direct responsibility for the regulatory system away from the entities being regulated.[36]

15.33 Proponents of principles-based regulation argue that, contrary to the assertions of clarity and certainty, rules-based regulation 'can be a dead hand on technology and product innovation'.[37] For example, the Parliamentary Secretary to the Treasurer, the Hon Chris Pearce MP, has argued that rules-based regulation introduces 'unnecessary legal complexity' and encourages 'box-ticking' exercises, rather than complying with the spirit and intent of the law.[38]

15.34 The disadvantages of a principles-based system centre on problems of ambiguity, which can undermine the system's intended protections and accountability:

> Principles are criticised for not providing certainty; for creating an unpredictable regulatory regime in which regulators can act retrospectively; for allowing firms to 'backslide', and get away with the minimum level of conduct possible; and thus for providing inadequate protection to consumers or others.[39]

15.35 Principles-based regulation often deals with this lack of clarity and certainty by integrating principles with other forms of regulation. For instance, detailed rules can be used to supplement principles; official guidelines can be issued to explain the principles; and dialogue can be facilitated between the regulator and regulated entities.[40]

15.36 Further, depending on the features of the regulatory scheme, principles-based regulation may also provide greater clarity through the interpretation of the principles by a regulatory body and the enforcement of those interpretations across the regulated industry or group.[41] This leads to the development of a body of precedent that clarifies the principles and provides entities with further guidance.

15.37 The emphasis on outcomes in principles-based regulation allows regulated entities to work towards the effective implementation of the principles within their own organisational context without dwelling on the 'expensive legislative focus'.[42] Thus, in the privacy law context, the Privacy Commissioner, Karen Curtis, stated:

---

35 See O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 331.

36 Investment and Financial Services Association, *Towards Better Regulation: Policy on Future Regulation of Financial Services in Australia* (2006), 3.

37 Ibid, 3, rec 1.

38 C Pearce, 'The Future of Governance Regulation in Australia' (Paper presented at 21st National Conference of Chartered Secretaries Australia, 22 November 2004).

39 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 2.

40 Ibid, 15.

41 An example is the United Kingdom's Financial Services Authority, as discussed in Ibid, 15 .

42 S Arjoon, 'Striking a Balance Between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68 *Journal of Business Ethics* 53, 82.

> By encouraging organisations to recognise the business advantages of good personal information handling practices and regulating their behaviour accordingly, government regulators can minimise regulatory intervention and red tape. This has been a common theme of our regulatory approach where a legislative framework is balanced by an emphasis on business privacy awareness and self-regulation. The idea is to inculcate the values and objectives of privacy law in business rather than just the superficial rules. When this happens organisations will be better equipped to deal with technological change because they will understand the ideas behind the laws—the principles—and will not become as confused by detailed technology-specific regulations. [43]

15.38 In this way, principles-based regulation aims to minimise the need for enforcement by 'encouraging organisations to understand the values behind the law and change their behaviour accordingly; not because they might get caught out by a regulator, but because they understand why the law is there and what its objectives are'.[44] This has been described as 'nurturing a culture of voluntary compliance with the law'.[45] Nevertheless, Black and others emphasise that breach of a principle should involve an element of fault and public sanction.[46]

15.39 Although rules-based and principles-based regulation are very different in their approach, in many instances the two systems can operate as a hybrid system, providing regulated entities with the benefits of both systems. In many established systems of regulation, high level principles that can be applied flexibly to new situations and promote a best practice approach to regulation are complemented by detailed rules providing clarity.

15.40 Currently, the IPPs and NPPs both represent hybrids, with each containing detailed rules and high level principles. For example, NPP 2 sets out relatively detailed rules related to the use and disclosure of personal information, whereas NPP 3 provides a broad, high level principle relating to data quality. An advantage of a hybrid system is that it seeks to take the advantages of both a principles- and a rules-based system in order to achieve regulatory clarity, enforceability and flexibility.[47]

---

43 K Curtis, 'Reducing Overlap, Duplication and Inconsistency' (Paper presented at Australian Regulatory Reform Evolution 2006, Canberra, 24 October 2006), 17.

44 Ibid, 13.

45 Australian Transactions Reports and Analysis Centre, *AUSTRAC Supervisory Framework* <www.austrac.gov.au/files/supervisory_framework.pdf> at 31 July 2007, 4.

46 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 4. See also Australian Transactions Reports and Analysis Centre, *AUSTRAC Supervisory Framework* <www.austrac.gov.au/files/supervisory_framework.pdf> at 31 July 2007, 4.

47 O Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 332.

Level of detail, guidance and protection

Background

15.41 In light of the above, it is necessary to consider how privacy should be regulated in the Act. This question was posed in the ALRC's Issues Paper, *Review of Privacy* (IP 31):

> Should federal privacy principles be prescriptive or should they provide high-level guidance only? Should they aim for a minimum or maximum level of protection of personal information or aim to adopt a best practice approach?[48]

15.42 An advantage of adopting high level principles is that they allow for greater flexibility, more easily accommodating unforeseen circumstances and a changing technological environment. For instance, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework expresses the view that the high level nature of the OECD Guidelines 'makes them still relevant today'.[49]

15.43 A disadvantage of high level principles, however, is that they can fail to provide adequate guidance. This in turn may promote a proliferation of guidelines and information sheets, which may not be legally binding. In contrast, detailed rules provide more guidance, thereby promoting certainty and consistency in application.

15.44 Generally worded, high level principles are usually considered 'light-touch' regulation because it is thought to be more difficult to establish a breach of such principles than provisions imposing detailed and specific obligations. At the time of introducing the private sector provisions of the *Privacy Act,* the then Attorney-General expressed an intention to make the Act responsive to business and consumer needs.[50] This was to be achieved, in part, by adopting high level principles rather than prescriptive rules.[51]

15.45 Another issue is whether the privacy principles should contain a minimum, intermediate or maximum level of protection of personal information. Commentators have noted that there is a choice between two broad dynamics in modelling privacy principles in a globalised environment:

> On the one hand, countries [could] progressively fashion their privacy protection policies according to the highest standard, a 'trading up' or a 'race to the top'. Conversely, countries might consider that a less-regulated climate would attract global business that would want to circumvent the higher standards at work elsewhere. This competitive deregulation would lead to a race to the bottom, as

48 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–36.
49 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), fn 1.
50 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General).
51 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 164.

countries progressively weaken their standards to attract global investment in the information technology and services industries.[52]

Submissions and consultations

Level of detail

15.46 A very large number of stakeholders favoured privacy principles that provide high level guidance, as distinct from prescribing in detail what is and is not permissible.[53] Some stakeholders emphasised that this permits greater flexibility for agencies and organisations.[54] One stakeholder submitted that this should be recognised more explicitly in the *Privacy Act*.[55] The Australian Government Department of Employment and Workplace Relations also submitted that the use of language that is not overly prescriptive will make it easier to move to a set of Unified Privacy Principles, applicable to the public and private sectors.[56]

15.47 Some stakeholders submitted that, by emphasising the objectives of the law rather than its detail, principles-based regulation tends to promote technological neutrality and makes the law more resilient to change.[57] It was submitted that this also aids in ensuring the law is clear and easy to apply.[58]

---

52 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), xv.

53 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

54 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

55 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

56 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

57 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

58 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

15.48 It was argued that principles-based regulation is more appropriate in a co-regulatory environment.[59] The Office of the Privacy Commissioner (OPC) stated:

> Principle-based law is aimed at encouraging organisations to understand the values behind the law and change their behaviour accordingly; not just to prevent action from being taken against them by a regulator, but because they understand why the law is there, what its objectives are and that it may benefit its business outcomes.[60]

15.49 Some stakeholders suggested that a balance should be struck between high level guidance and the more detailed prescription associated with traditional legislative regulation.[61] Others suggested that it is necessary to adopt a more prescriptive approach. Professor William Caelli submitted:

> Privacy Principles MUST be prescriptive or else they will be largely ignored … There is no evidence that the private or public sector alike have embraced advanced information security systems WITHOUT legal obligation. This could also be clearly stated even for many matters of safety, eg, seat belts being made compulsory for inclusion in any manufactured or imported car, etc.[62]

15.50 Similarly, the National Health and Medical Research Council (NHMRC) submitted that the current high-level privacy principles have 'led to a proliferation of long, complex and often unclear guidelines and information sheets'. It argued that, at least in the health and research context, this can

> confuse stakeholders, leading many to adopt a highly conservative approach to compliance, with negative consequences for the clinical care of some individuals and for the conduct of some high quality health and medical research.[63]

15.51 On the other hand, the Northern Territory Information Commissioner submitted that some level of 'uncertainty' is the price that must be paid for allowing 'flexibility for agencies and organisations to protect privacy according to the particular context in which they operate'.[64]

15.52 The NHMRC further argued that more prescriptive privacy principles would 'aid understanding and compliance'. For instance, if further attention were paid in the principles to the consequences of a data breach, this would 'ensure that penalties are proportionate to the significance of the breach'.[65]

---

59 Ibid; Law Council of Australia, *Submission PR 177,* 8 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

60 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

61 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

62 W Caelli, *Submission PR 99,* 15 January 2007.

63 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

64 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

65 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007. Note that the issue of data breach is dealt with in Part F of this Discussion Paper.

Minimum standards or maximum protection?

15.53 A number of stakeholders submitted that the privacy principles should continue to articulate minimum standards, as distinct from attempting to provide maximum privacy protection.[66] Some stakeholders linked this with the intention to adopt a 'light-touch' regulatory approach.[67] The Australian Bankers' Association argued that the current approach is working well and that those who favour more onerous regulation should first be required to 'establish the case for additional regulation and to demonstrate the benefits'.[68] It was also noted that, if more onerous obligations were imposed, this would strengthen arguments for retaining an exemption for small businesses in the *Privacy Act*.[69]

15.54 While acknowledging the importance of having privacy principles, a number of stakeholders noted that this does not preclude some aspects of privacy from being regulated in a more prescriptive manner, where this is required by the particular situation.[70] The OPC observed that the NPPs and IPPs were always intended to be 'minimum standards' that ought properly to be supplemented in appropriate circumstances.[71] Similarly, other stakeholders observed that the current approach whereby the IPPs and NPPs are supplemented by Codes of Practice and other guidance operates effectively.[72]

15.55 Some stakeholders argued that it is desirable to establish privacy principles that promote best practice.[73] Electronic Frontiers Australia, for instance, asserted that the

---

66 Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

67 Veda Advantage, *Submission PR 163,* 31 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

68 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also Government of South Australia, *Submission PR 187,* 12 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

69 Government of South Australia, *Submission PR 187,* 12 February 2007. The exemptions in the *Privacy Act* are discussed in Part E of this Discussion Paper.

70 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

71 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

72 Veda Advantage, *Submission PR 163,* 31 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

73 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

current approach is 'inadequate' in providing privacy protection.[74] The NHMRC argued, however, that this should still aim to balance 'the dual objectives of protecting individual privacy and promoting the public interest by enabling access to information for public benefit in appropriate circumstances'.[75]

ALRC's view

Level of detail

15.56 The fact that a very large number of stakeholders supported the use of high level principles in the *Privacy Act* reflects that this clearly remains the preferred system to regulate privacy when compared with more detailed, prescriptive legislation. Similarly, other jurisdictions continue to favour principles-based regulation to protect information privacy. For example, a 2006 report in the United Kingdom that focused on the impact of surveillance on privacy reached the following conclusion:

> We are not persuaded that, in searching for regulatory solutions to surveillance, the baby should be thrown out with the bath water; or, to change the liquid metaphor, that privacy principles and regimes are now, like King Canute, incapable of holding back a supposed flood of surveillance. The set of 'fair information' data protection principles is the only reasonably structured, systematic and practically oriented ethical framework currently available.[76]

15.57 The ALRC is also of the view that a principles-based approach should continue to be at heart of the *Privacy Act*, and that this should remain the starting point for the regulation of privacy. The ALRC favours such an approach because it is more flexible and adaptable to the multitude of circumstances in which agencies and organisations must take account of individuals' privacy rights. These features make the *Privacy Act* more resilient to change, especially in response to technological developments that impact on privacy.

15.58 However, as is noted above and is illustrated in greater detail in the following chapters in Part D, the IPPs and NPPs are not exclusively constituted by archetypal principles. Some of the provisions—such as IPP 9 and NPP 8—are relatively brief, expressing broad and general obligations or objectives to be achieved. On the other hand, principles such as IPP 5 and NPP 2 are more detailed, specifying with greater precision the obligations that apply in the relevant circumstances. In other words, the IPPs and NPPs represent a compromise. This means that, for certain provisions, it was deemed desirable to adapt the conventional principle structure, expressing the relevant obligations more prescriptively and in greater detail.

15.59 The ALRC believes that this compromise approach is desirable because, by eschewing a doctrinaire adherence to any particular regulatory theory, Parliament is

---

74 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

75 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007

76 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, 80.

able to respond more flexibly to the needs of individuals, agencies and organisations at the various stages of the information cycle. The ALRC believes that relying solely on either rules- or principles-based regulation would not provide agencies and organisations with sufficient flexibility or security in their interpretation and implementation of privacy policies. Therefore, the ALRC is of the view that the continuation of a hybrid regulatory scheme will allow agencies and organisations to understand the purpose of the law and to drive organisational behaviour towards best practice. The overall regulatory structure should provide more detailed guidance and regulation where it is necessary to deal with particular issues.

15.60 Consequently, the ALRC's proposes that the obligations in the privacy principles generally should be expressed as high level principles. However, this should remain a broad objective, rather than a strict rule, in the drafting of the privacy principles. Care should also be taken, therefore, to ensure that the privacy principles are simple, clear and easy to understand and apply.

Minimum standards or maximum protection?

15.61 As explained above, the ALRC believes that privacy should generally be regulated in the *Privacy Act* by high level principles that set out the objectives to be achieved by agencies and organisations, usually without specifying in detail how this should be carried out. This approach is clearly inconsistent with legislation that seeks to articulate a detailed, prescriptive set of minimum *requirements* applicable to agencies and organisations. However, this does not answer the question whether the Act should set out minimum or maximum *standards*.

15.62 There is a longstanding policy position that the *Privacy Act* should be light-touch, in the sense that it should provide only such regulation as is required to protect individuals' privacy without unreasonably burdening the public or private sectors. The ALRC reiterates this position and, to further this goal, the ALRC believes the privacy principles should contain reasonable obligations that provide adequate protection of individuals' privacy rights and help to promote best practice, without creating an excessive compliance burden.

15.63 Moreover, formulating the privacy principles must involve a careful balance between competing considerations to determine how best to maximise public benefit. To this end, Professor Fred Cate has stated:

> Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and individual privacy have value and are necessary in a democratic society and market economy. That value benefits individuals as well as society as a whole. Therefore, the goal of any privacy regime must be to balance the

> value of accessible personal information with the value of information privacy to maximize both individual and public benefits.[77]

15.64 The ALRC's preferred approach is to avoid trying to impose a 'one-size-fits-all' solution. In certain areas, it may be necessary to provide more detailed regulation that imposes either stricter or more lenient obligations.[78] As Black argues, 'the advantages and disadvantages of certain types of rules [are not] the same for all actors in the regulatory regime'.[79] Consequently, the ALRC is of the view that the optimum approach to the drafting of the privacy principles is to establish reasonable obligations on agencies and organisations. These obligations would generally apply to all agencies and organisations. In some situations, however, the obligations in the privacy principles will be displaced by more specific obligations that apply in a particular area—for instance, in credit reporting, health research and treatment, and in the telecommunications industry.[80]

Proposal 15–1 The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

(a) the obligations in the privacy principles generally should be expressed as high level principles;

(b) the privacy principles should be simple, clear and easy to understand and apply; and

(c) the privacy principles should impose reasonable obligations on agencies and organisations.

Towards a single set of privacy principles

Background

15.65 A question arises as to whether it is preferable to maintain two separate sets of similar, but sometimes inconsistent, privacy principles, or to create a unified set of privacy principles (the Unified Privacy Principles or UPPs). The ALRC asked in IP 31 whether the IPPs and NPPs should be consolidated to create a single set of privacy principles applicable to both the public and private sectors and, if so, what model

---

77 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 29.

78 See, eg, the discussion in Ch 23 of the differing forms of regulation, and standards, for the various types of direct marketing.

79 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 12.

80 For those more detailed requirements, see Parts G, H and J of this Discussion Paper.

should be used. A related question was asked as to whether any particular principles, or exceptions to principles, should apply only to either the public or private sector.[81]

15.66 As noted above, the OECD Guidelines apply to personal data in both the public and private sectors. Consequently, there is no reason to presume that it is necessary to establish two sets of privacy principles for the public and private sectors in order to implement the OECD Guidelines. Similarly, the principles in the APEC Privacy Framework and in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive) also apply to both the public and private sectors.[82]

15.67 There is precedent in other jurisdictions for having a single set of principles applying both to the public and private sectors,[83] as well as for having separate principles or provisions regulating the public and private sectors.[84]

15.68 One problem with the current system is that there are circumstances when an organisation or agency is subject to both the IPPs and the NPPs. For example, an Australian Government contractor may be bound to under the Act to comply with the NPPs but may also be bound by contract to comply with the IPPs.[85] Some government business enterprises—such as Australia Post—are, for the purposes of the *Privacy Act*, both an agency in respect of their non-commercial activities, and an organisation in respect of their commercial activities.[86]

15.69 In determining the most appropriate 'model' for a unified set of privacy principles, it is necessary to consider a number of related questions—some of which are addressed in this Part, some of which are addressed elsewhere. Those questions include:

- What should be the general structure of a single set of privacy principles? This question is addressed earlier in this chapter.

- What should be the content of a single set of privacy principles? This question is addressed in the remaining chapters in this Part.

---

81 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–34.

82 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005); European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

83 See, eg, *Privacy Act 1993* (NZ); *Data Protection Act 1998* (UK); *Personal Data (Privacy) Ordinance* (Hong Kong).

84 See, eg, *Privacy Act* RS 1985, c P-21 (Canada) (regulation of public sector); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) (regulation of private sector).

85 See *Privacy Act 1988* (Cth) ss 95B, 6A(2).

86 Australia Post, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004. See *Privacy Act 1988* (Cth) s 7(c); *Freedom of Information Act 1982* (Cth) sch 2, div 1, pt II.

- In the event that a single set of privacy principles is adopted, is it necessary to create a further layer of more detailed regulation that would apply to certain spheres or activities? This general question is considered in Part F. In later chapters, this Discussion Paper addresses how this proposal might operate in certain specific areas—such as health and research,[87] credit reporting[88] and telecommunications.[89]

Previous privacy inquiries

15.70 The question whether to move to some form of unified privacy principles has been the subject of considerable debate in previous privacy inquiries.[90] In 2005, the OPC expressed its preference for a single set of principle principles:

> There seems no clear rationale for applying similar, but slightly different, privacy principles to public sector agencies and private sector organisations and certainly no clear rationale for applying both to an organisation at the same time. There is no clear policy reason why they are not consistent. The time may have come for a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations.[91]

15.71 The OPC recommended that:

> The Australian Government should consider commissioning a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations. This would address the issues surrounding Australian Government contractors.[92]

15.72 Submissions to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth) (Senate Committee privacy inquiry) and to the Taskforce on Reducing Regulatory Burdens on Business expressed concern about the inconsistency within the *Privacy Act* resulting from two sets of principles.[93] It was also

---

87 See Part H.
88 See Part G.
89 See Part J.
90 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006).
91 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46.
92 Ibid, rec 5. The Taskforce on Reducing Regulatory Burdens on Business came to a similar conclusion. See Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.
93 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.35]; Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 56.

noted that two separate regimes caused particular difficulties in the health sector, where public and private health organisations often work closely together.[94]

15.73 The Senate Committee privacy inquiry ultimately recommended that the ALRC develop a single set of privacy principles:

> The committee recommends the development of a single set of privacy principles to replace both the National Privacy Principles and Information Privacy Principles, in order to achieve consistency of privacy regulation between the private and public sectors. These principles could be developed as part of the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2.[95]

Submissions and consultations

Support for single set of privacy principles

15.74 A very large number of stakeholders submitted that it would be desirable to consolidate the IPPs and NPPs to create a single set of privacy principles, which would be generally applicable to organisations and agencies.[96] The basis for supporting a move to the UPPs derives both from problems with having separate sets of privacy principles for the public and private sectors, as well as positive outcomes that could be achieved through a single set of principles.

15.75 Stakeholders were particularly concerned that maintaining separate sets of privacy principles—the NPPs and IPPs—creates complexity and confusion in a number of areas, including:

---

94 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.37].

95 Ibid, rec 4, [7.9].

96 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Law Institute of Victoria, *Submission PR 200,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; Australian Health Insurance Association, *Submission PR 161,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; National E-health Transition Authority, *Submission PR 145,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Australia Post, *Submission PR 78,* 10 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; National and State Libraries Australasia, *Submission PR 68,* 21 December 2006; The Mailing House, *Submission PR 64,* 1 December 2006.

- for consumers, because the differential privacy standards can make it difficult for an individual to know what are their privacy rights in any given situation;[97]

- for staff of organisations and agencies, who are required to determine which privacy principles apply and when;[98]

- the often subtle differences in the requirements of the IPPs and NPPs, which can create conflicting or overlapping requirements;[99] and

- in public-private partnerships, or in respect of other entities that must comply with both the IPPs and NPPs.[100] In these situations, it can increase the cost of compliance because two compliance regimes need to be established and it is sometimes unclear precisely when the IPPs apply and when the NPPs apply.[101]

15.76 Positive reasons were also advanced for the establishment of the UPPs. For instance, it was submitted that this would help achieve the desirable goals of national consistency,[102] as well as consistency with a number of the key international instruments such as the EU Directive, the OECD Guidelines and the APEC Privacy Framework.[103] It was also submitted that this would simplify compliance requirements and, therefore, enhance administrative convenience.[104] Moreover, any compliance

---

97 Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; AAMI, *Submission PR 147,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

98 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

99 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

100 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Law Institute of Victoria, *Submission PR 200,* 21 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

101 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

102 Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.

103 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

104 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

burden associated with introducing the new UPPs would be offset by savings from no longer having to maintain two separate privacy regimes.[105] The OPC further submitted that the number of similarities between the IPPs and NPPs appear to make the task of rationalisation feasible.[106]

Opposition to single set of privacy principles

15.77 A significant, though smaller, number of stakeholders opposed moving to a single set of privacy principles.[107] The Australian Bankers' Association was concerned that moving now to a single set of privacy principles would be 'premature', given that the NPPs were only recently enacted.[108] It noted that many organisations have already 'invested significant amounts of time and money in developing their compliance arrangements to ensure their compliance with the Act' and that moving to a single set of principles would require further expenditure at a time when it appears that the NPPs are working satisfactorily.[109]

15.78 Some stakeholders focused on the fact that sometimes it is necessary to impose different requirements on organisations and agencies.[110] Specifically, there was concern that the objects and functions of agencies differ from those of organisations and so it is appropriate to impose differing privacy requirements on each.[111] For example, special principles may need to apply to the public sector because it can compel the production of personal information.[112] It was also suggested that it may be necessary to create a specific principle dealing with direct marketing that should apply only to the private sector—that is, it should not apply to agencies.[113]

15.79 Some alternatives were suggested to the establishment of the UPPs. For instance, the IPPs and NPPs could be amended, where appropriate, to enhance their consistency.[114] Another alternative would be to amend the *Privacy Act* to state that the

---

105 See, eg, National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

106 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

107 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Confidential, *Submission PR 165,* 1 February 2007; AXA, *Submission PR 119,* 15 January 2007.

108 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

109 Ibid. See also AXA, *Submission PR 119,* 15 January 2007.

110 It should be noted, however, that some stakeholders argued that such inconsistencies as these could be accommodated by the *Privacy Act*: see Law Institute of Victoria, *Submission PR 200,* 21 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

111 Confidential, *Submission PR 165,* 1 February 2007.

112 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Confidential, *Submission PR 165,* 1 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

113 Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006. Direct marketing is dealt with in Ch 23.

114 Australian Federal Police, *Submission PR 186,* 9 February 2007.

NPPs apply to all personal information provided by a government agency under a service contract.[115]

ALRC's view

15.80 The overwhelming majority of stakeholders who expressed a view on this issue were in favour of consolidating the IPPs and NPPs to create a single set of privacy principles that would be generally applicable to organisations and agencies. There was also a consensus among each of the various categories of stakeholder—that is, among organisations, agencies and others. The ALRC shares this view and believes that the IPPs and NPPs should be consolidated to establish the UPPs that would be generally applicable to agencies and organisations.

15.81 A large number of benefits would flow from such a reform. For instance, the move to a set of UPPs would foster national and international consistency in privacy regulation.

15.82 Such a reform would also clarify and simplify the obligations of agencies and organisations with respect to information privacy. This would be advantageous to individuals who interact with these entities, and also for the agencies and organisations themselves, as they would not have to differentiate between the overlapping requirements of the IPPs and NPPs. Where an organisation is acting as a contracted service provider or it is involved in a public-private partnership, it would significantly reduce the problems associated with the organisation having to comply with both the IPPs and NPPs. This simplification would be likely to offset costs associated with implementing a new regime for privacy regulation.

15.83 The ALRC does not believe, however, that the UPPs should apply rigidly to agencies and organisations. As explained in the remaining chapters in this Part, some privacy principles should incorporate provisions that apply exclusively to agencies or organisations, and indeed some principles in the UPPs should apply only to organisations.[116] Moreover, the ALRC is of the view that the UPPs should apply except to the extent that more specific primary or subordinate legislation covers a particular aspect of privacy or handling of personal information.

15.84 Adopting such an approach responds to a persistent concern among those opposed to a single set of privacy principles—namely, that this would not adequately address the fundamental differences between agencies and organisations. That is, the UPPs will be sufficiently flexible to differentiate, where appropriate, between the information privacy obligations that apply to agencies and organisations.

---

115 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

116 See Chs 23, 26.

Proposal 15–2 The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles—the Unified Privacy Principles (UPPs)—that would be generally applicable to agencies and organisations, subject to such exceptions as required.

Proposal 15–3 The proposed UPPs should apply to information privacy except to the extent that:

(a) the *Privacy Act* or another piece of Commonwealth primary legislation imposes different or more specific requirements in a particular context; or

(b) subordinate legislation under the *Privacy Act* imposes different or more specific requirements in a particular context.

Scope and structure of Unified Privacy Principles

Scope of Unified Privacy Principles

15.85 In considering the content of the privacy principles, the first question is: what should be the scope of the UPPs? In other words, should the scope of the UPPs match that of the IPPs, NPPs or both; or should the scope be narrower or broader?

15.86 Taken together, the IPPs and NPPs cover the following aspects of privacy in relation to personal information: collection; use and disclosure; data quality; data security; openness; access and correction; the use of identifiers; the principle of anonymity; the regulation of transborder data flows; and the special protections that should apply to particularly sensitive information.

15.87 The ALRC believes that, at a minimum, the UPPs should cover the same aspects of privacy as are currently covered by the IPPs and NPPs, when taken together. There are a number of reasons why the ALRC takes this view. First, this coverage is broadly consistent with the privacy regimes of other jurisdictions and at international law. Secondly, this will allow the *Privacy Act* to derogate, where appropriate, from the general provisions of the UPPs. The question whether the scope of the UPPs should be expanded to cover additional aspects of privacy is addressed in Chapter 29.

Structure of a single set of privacy principles

15.88 Assuming the IPPs and the NPPs are consolidated to create a single set of privacy principles (the UPPs), a question arises as to how the UPPs should be structured. Specifically, should the UPPs be based on the NPPs, the IPPs or neither?

15.89 A number of stakeholders have expressed the view that the NPPs—though capable of improvement—are superior to the IPPs and should form the model for any set of UPPs.[117] It was noted that this would reduce the cost of compliance for the private sector.[118]

15.90 The privacy statutes of Victoria, Tasmania and the Northern Territory are largely based on the NPPs—although they are not 'word for word' replicas.[119] In each case, the NPPs have been used as a basis for the principles that are to apply to public sector bodies—although the Tasmanian provisions also apply to 'any body, organisation or person who has entered into a personal information contract relating to personal information'.[120] On the other hand, the privacy legislation of New South Wales and the privacy schemes in Queensland and South Australia resemble more closely the IPPs.[121] It was noted, however, that South Australia's Department of Health and Department for Families and Communities have both adopted the NPPs, which 'demonstrat[es] the ability of the NPPs to be applied in a public sector setting'.[122]

15.91 Some stakeholders stated that, if there were to be one set of privacy principles, it would be preferable to develop a new set of principles rather than merely merging and modifying the existing NPPs and IPPs.[123] The OPC argued that the NPPs are

> concise and more user friendly … [than] the IPPs. This is due in part to the fact that the NPPs were developed with the consideration that they must cater to a wider range of organisations, from individual health providers to large corporations and therefore were required to be easier to apply in a variety of situations. Similarly, the drafting language of the NPPs utilises plain English in comparison to the earlier drafted IPPs.[124]

15.92 One key consideration in determining the model of privacy principles to be applied is the compliance burden and costs that will be imposed on agencies and organisations who have set up compliance systems in response to the requirements imposed by the IPPs and the NPPs. Departing radically from those principles would increase the consequential compliance burden imposed on those entities that are subject to the UPPs. The OPC concluded that the NPPs 'have worked well and

---

117 See, eg, Government of South Australia, *Submission PR 187,* 12 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; AAMI, *Submission PR 147,* 29 January 2007; D Antulov, *Submission PR 14,* 28 May 2006.

118 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

119 See *Information Privacy Act 2000* (Vic) sch 1; *Personal Information Protection Act 2004* (Tas) sch 1; *Information Act 2002* (NT) sch 2.

120 See *Personal Information Protection Act 2004* (Tas) s 3.

121 See *Privacy and Personal Information Protection Act 1998* (NSW) pt 2, div 1; Queensland Government Department of Justice and Attorney-General, *Privacy* (2005) <www.justice.qld.gov.au/dept/privacy.htm> at 31 July 2007; South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

122 Government of South Australia, *Submission PR 187,* 12 February 2007.

123 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.

124 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

delivered to individuals protection of personal and sensitive information in Australia in those areas covered by the Act'.[125] However, as noted above, the Senate Committee privacy inquiry disagreed with the OPC's conclusion that the private sector provisions are 'working well'.[126]

ALRC's view

15.93 The ALRC's view is that the general structure of the NPPs has been largely effective. This is borne out by the response of stakeholders to this Inquiry, the majority of whom have indicated that they are generally satisfied with how the NPPs are structured. It is also noted that to adopt a radically different structure from the NPPs would involve a greater compliance burden, particularly on organisations that have to update their privacy protection regimes.

15.94 Consequently, assuming Proposal 15–2 is adopted, the ALRC believes that the NPPs should form the general template in drafting and structuring the UPPs. In making this proposal, two important points should be made. First, this proposal is not intended to impact on the *substantive content* of the UPPs; rather it is intended only to guide the *general form* or framework of the UPPs. Secondly, the ALRC does not propose that the statutory draftspersons should slavishly follow the NPP structure or wording where it is obvious that amendments can be made that would improve on the status quo. Instead, it would be entirely appropriate for the UPPs to depart from the general structure of the NPPs in such circumstances. This general approach is reflected in the way in which the proposed UPPs have been drafted by the ALRC in this Discussion Paper.[127]

Proposal 15–4 The National Privacy Principles should provide the general template in drafting and structuring the proposed UPPs.

125 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 2–3.

126 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.27].

127 The proposed UPPs are set out at the beginning of this Discussion Paper.

16. Consent

Contents

Introduction 571
'Consent' and 'bundled consent' in the *Privacy Act* 572
Background 572
Submissions and consultations 573
ALRC's view 576
A separate privacy principle dealing with consent? 583
Background 583
Submissions and consultations 584
ALRC's view 584

Introduction

16.1 This chapter considers the issue of consent as it applies to the privacy principles in the *Privacy Act 1988* (Cth). The fact that an individual has provided consent to the handling of his or her personal information can—in some circumstances under the National Privacy Principles (NPPs), Information Privacy Principles (IPPs) and proposed Unified Privacy Principles (UPPs)—provide lawful authority to the relevant agency or organisation to deal with the individual's personal information in that way.

16.2 This chapter focuses on three main questions. First, should the definition of 'consent' in the *Privacy Act* be amended? Secondly, should the Office of the Privacy Commissioner (OPC) provide further guidance as to the meaning of consent? Thirdly, should the proposed UPPs contain a separate principle that deals with the issue of consent?

16.3 The term 'consent' is defined in the *Privacy Act* to mean 'express consent or implied consent'.[1] In relation to implied consent, the OPC has noted that this can be inferred from an individual's 'failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up'.[2]

16.4 Whether an individual has given his or her consent can be critical in determining whether an agency or organisation should be permitted to use or disclose the

1 *Privacy Act 1988* (Cth) s 6(1).
2 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 37.

individual's personal information. For example, NPP 2.1(b) provides that organisations may use or disclose personal information for a secondary purpose if the individual has consented to the use or disclosure. Similar provisions apply in the IPPs in respect of agencies.[3] The NPPs also contain exceptions relating to consent in respect of transborder data flows and the collection of sensitive information. That is, an organisation is permitted to transfer an individual's personal information to a foreign country if the individual consents to the transfer,[4] and the general prohibition on an organisation collecting sensitive information does not apply where the individual has consented.[5]

'Consent' and 'bundled consent' in the *Privacy Act*

Background

16.5 As noted above, there are exceptions to the use and disclosure restrictions under the IPPs and NPPs where the individual in question consents to the use or disclosure. Problems arise where an individual's capacity to give true consent—that is, to make an informed and free choice—is hampered. This issue is seen most commonly in the context of 'bundled consent'. Bundled consent refers to the practice of an agency or organisation 'bundling together', or consolidating, multiple requests for individuals' consent to a wide range of uses and disclosures of personal information, without giving individuals the option of selecting to which uses and disclosures they agree. Bundled consent is often sought as part of the terms and conditions of a product or service.[6]

16.6 Submissions from consumer groups to the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) were highly critical of the practice, stating, for example, that it undermines the requirement that consent be meaningful, informed and freely given.[7] Similar sentiments were expressed in some submissions to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry). For example, one stakeholder stated that it was difficult for individuals to give free and informed consent when presented only with broad or vague statements concerning possible uses and disclosures, or when told that services would not be provided in the absence of consent.[8]

16.7 On the other hand, there may be legitimate circumstances in which organisations seek bundled consent from consumers.[9] Submissions from the business sector, and particularly the finance and telecommunications industries, to both the OPC Review

---

3 See *Privacy Act 1988* (Cth) s 14, IPPs 10.1(a) and 11.1(a).
4 Ibid sch 3, NPP 9(b).
5 Ibid sch 3, NPP 10.1(a).
6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 82.
7 Ibid, 85.
8 See Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.140]–[4.141].
9 Note that concerns relating to bundled consent in the context of credit reporting and telecommunications are addressed respectively in Parts G and J of this Discussion Paper.

and the Senate Committee privacy inquiry emphasised the need to seek bundled consent in order to achieve business efficiency and to reduce costs to the consumer. For example, telecommunications organisations submitted that to obtain consent for each specific use of an individual's personal information would significantly increase the complexity and costs of compliance. These costs, they argued, would inevitably be passed on to the consumer.[10] Vodafone submitted to the OPC Review that unbundling consent would have negative outcomes for consumers and suppliers, by increasing the volume and frequency of communications.[11] Submissions from the finance industry emphasised that seeking a single consent for multiple uses of information—for example, in an application for finance—was necessary to ensure that the information could be used not only to process the application, but to manage the account, administer insurance claims, recover money owed and maintain the value of the asset.[12] In 2005, the OPC stated that it would develop guidelines on bundled consent.[13]

16.8 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked the following question:

> Are there particular issues or concerns arising from the practice of organisations seeking bundled consent to a number of uses and disclosures of personal information? If so, how are these concerns best addressed?[14]

Submissions and consultations

16.9 A large number of stakeholders expressed concern about the use of bundled consent. It was noted that this requires individuals to adopt an all or none approach—that is, they are unable to specify what particular uses or disclosures are and are not acceptable to them.[15] Some stakeholders argued simply that this area of law needs to be clarified.[16]

16.10 Several examples were given of problems arising from agencies or organisations using bundled consent. These include:

---

10 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 86. See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.142]–[4.143].

11 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 86.

12 Ibid, 86.

13 Ibid, rec 22.

14 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–11.

15 See, eg, Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Anglicare Tasmania, *Submission PR 135,* 19 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

16 See, eg, G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

- internet sites often require bundled consent before one can enter the site;[17]

- a particular real estate agent is said to use a single form to request a prospective tenant's consent to the disclosure of personal information to the media, the landlord, residential tenancy databases and the local real estate industry body, even though each of these entities would use the information differently and for differing purposes;[18] and

- sometimes the language used in a bundled consent form is 'particularly inaccessible for people with literacy issues and those for whom English is a second language'.[19]

16.11 The OPC maintained that 'consent is a cornerstone of privacy' and involves two critical elements: (a) consent must be informed, so that an individual knows to what he or she is agreeing; and (b) a request for consent must give an individual 'real choice'.[20]

16.12 A critical stumbling block in relation to bundled consent is where a failure to provide consent leads to an agency or organisation withholding access to a good or service. A number of stakeholders expressed concern about this,[21] and some argued that it should be prohibited.[22] AAMI, for instance, suggested that this practice is unfair and punitive, and may be unlawful under the *Fair Trading Act 1999* (Vic).[23] The NSW Disability Discrimination Legal Centre was concerned that this could lead to individuals refusing to give consent (and thereby not accessing the relevant service) because they fear that this may allow their sensitive information to be used against them at some stage in the future.[24]

16.13 On the other hand, some stakeholders observed that sometimes an agency or organisation needs to use or disclose an individual's personal information to enable it to provide a particular service. If this is the case, it should be permitted to withhold the service unless consent is provided.[25] The OPC seems to have taken a middle line, suggesting that

---

17 AAMI, *Submission PR 147,* 29 January 2007.
18 Anglicare Tasmania, *Submission PR 135,* 19 January 2007.
19 Ibid. See also Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
20 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A similar approach was taken by: Veda Advantage, *Submission PR 163,* 31 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.
21 See, eg, Confidential, *Submission PR 143,* 24 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
22 See, eg, AAMI, *Submission PR 147,* 29 January 2007.
23 Ibid.
24 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.
25 Law Council of Australia, *Submission PR 177,* 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

> where an agency or organisation wants to use information for a purpose other than [the purpose] for which it was collected, then the individual's consent should be sought for the extended use of that information but it should not be made a condition of the original service.[26]

16.14 Some stakeholders submitted that bundling consent—though perhaps not ideal in a perfect world—is necessary for practical reasons. This may be because an organisation or agency has multiple interactions with an individual client and must therefore handle the individual's personal information many times.[27] It may also be due to the practical necessity of outsourcing parts of a business, which leads to a greater number of entities handling an individual's personal information.[28] It was also pointed out that bundled consent can help to cut red tape and allow an individual to access a service more quickly.[29]

16.15 The Australian Bankers' Association submitted that at the heart of the bundled consent issue was the need to strike an appropriate balance between responding to statutory use and disclosure obligations and respecting individuals' information privacy requirements. It suggested that, at least in relation to the activities of its members, bundled consent might present a more theoretical than practical problem to individuals.[30]

16.16 Some stakeholders that accepted the need for bundled consent, at least in some circumstances, made suggestions to reform the bundled consent process. These included:

- where an individual is requested to consent to multiple items, these items should be 'directly related (as in primary and secondary purposes)';[31]
- the OPC should provide guidance on how and when to seek bundled consent;[32]

---

26 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

27 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

28 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

29 Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

30 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

31 AAMI, *Submission PR 147,* 29 January 2007.

32 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Anglicare Tasmania, *Submission PR 135,* 19 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

- organisations should be encouraged to move consent clauses from the terms and conditions of service into application forms;[33]

- the categories of personal information and the purposes for which they will be used should be clear at the outset and, if an agency or organisation wishes to deviate from this, it must explain this to the individual and obtain the individual's consent;[34]

- it should be made clear to individuals what are the things to which they are consenting;[35]

- an agency or organisation should not use a bundled consent form for things that are not genuinely necessary for the entity's interaction with the individual—for instance, it is inappropriate to use a bundled consent in respect of direct marketing;[36] and

- bundled consent may not be appropriate in respect of sensitive information, such as health information.[37]

ALRC's view

Meaning of 'consent'

16.17 The issue of consent—and, in particular, what is required to demonstrate that consent has been obtained and when consent should be required from a data subject—remain vexed issues in the context of privacy regulation. This is notwithstanding that, as noted above, the OPC has provided guidance on this subject and recommendations have been made by the OPC and the Senate Committee privacy inquiries to clarify the rules on consent.

16.18 The dictionary meaning of consent is 'to give assent; agree; comply or yield'.[38] This necessarily implies an element of voluntariness; otherwise the concept is indistinguishable from passive acceptance.

16.19 The ALRC is of the view that the specific requirements of consent—particularly as regards the requisite level of voluntariness—are highly dependent on the context in which the personal information is collected, used or disclosed. In other words, what

---

33 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
34 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.
35 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.
36 Law Council of Australia, *Submission PR 177,* 8 February 2007.
37 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.
38 *Macquarie Dictionary* (online ed, 2005).

may be required to obtain consent in one situation may differ, sometimes significantly, from what is required to obtain consent in another situation.

16.20 Take the following hypothetical example. An organisation has a large number of customers from a particular ethnic group. The organisation wishes to create a customer database using personal information about its customers, including their home addresses, and this database will help the organisation deliver a service to its customers. If the individual customers approve of this use of their home addresses, the information will likely be innocuous. If, however, the organisation intends to sell the contents of this database to another entity—perhaps one that is engaged in direct marketing or, more worryingly, a racist group that is looking to target members of that particular ethnic group—this same information would take on a different significance. In the latter circumstances, knowing precisely how his or her personal information is to be used or disclosed will have a critical impact on whether the individual consents to that use or disclosure.

16.21 The importance of context in any analysis of privacy, and particularly in maintaining control over personal information, was highlighted by Callinan J in *Australian Broadcasting Corporation v Lenah Game Meats*:

> Privacy is necessary for the formation of intimate relationships, allowing us to reveal parts of ourselves to friends, family members, and lovers that we withhold from the rest of the world. … In *The Unbearable Lightness of Being*, Milan Kundera describes how the police destroyed an important figure of the Prague Spring by recording his conversations with a friend and then broadcasting them as a radio serial. Reflecting on his novel in an essay on privacy, Kundera writes, 'Instantly Prochazka was discredited: because in private, a person says all sorts of things, slurs friends, uses coarse language, acts silly, tells dirty jokes, repeats himself, makes a companion laugh by shocking him with outrageous talk, floats heretical ideas he'd never admit in public, and so forth.'[39]

16.22 This emphasises that, in order to protect an individual's privacy, it is necessary to give careful consideration to context. This point is heightened when considering whether a person has consented to a particular use or disclosure. Clearly, an individual should not be expected to give consent to a data collector in respect of any use of his or her personal information that the data collector considers appropriate. Rather, consent should involve the individual being adequately informed, before giving consent, of the circumstances, nature and basis of the proposed use. Equally, however, the level of effort that a data collector should be expected to undertake to secure the consent of an individual also will depend on these contextual factors.

---

39 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [321], citing J Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2000), 11.

16.23 The ALRC notes that there is a clear desire from a large number of stakeholders for greater clarity as to the meaning of 'consent' more generally. In approaching this issue in the context of the *Privacy Act*, the ALRC believes that the OPC's existing guidance on this issue provides a useful starting point.[40]

16.24 In articulating the general meaning of consent in privacy law, it is also useful to refer to other jurisdictions. For example, the *Model Code for the Protection of Personal Information*, which is set out in Canada's *Personal Information Protection and Electronic Documents Act 2000* (PIPED Act), states that, in obtaining consent, the reasonable expectations of the individual are relevant. The Model Code also states that generally organisations should seek express consent when the information is likely to be considered sensitive, and that implied consent would generally be appropriate when the information is less sensitive.[41] This reflects a contextual approach to the issue of consent in privacy law. The draft Asia-Pacific Privacy Charter is more prescriptive, stating that consent should be 'freely-given, informed, variable and revocable'. It states that consent is 'meaningless if people are not given full information, or have no option but to consent in order to obtain a benefit or service'.[42]

16.25 Taking account of how consent has been interpreted in Australia and overseas, the ALRC believes that there are four critical factors that apply in the privacy area when considering whether an individual consents to the handling of his or her personal information in a given situation:

- The context in which the consent is sought—this means considering how the consent is sought; the characteristics of the individual from whom consent is sought; the thing(s) to which the individual appears to be giving his or her consent; and any other relevant factors.

- Whether there is informed consent—this requires an analysis of the individual's likely level of understanding as to what he or she is consenting to, and the implications of giving and withholding his or her consent. As explained in the 2003 report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), it is critical for an individual to be 'given sufficient information to enable [him or her] to make an informed decision' as to whether to give consent.[43]

---

40 See Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 38. The relevant part of these Guidelines is extracted later in this chapter.

41 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.36.

42 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, Principle 2.

43 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.27]

- Whether the consent is voluntary—this requires an analysis of whether the individual has a clear option not to consent, and whether receiving the opportunity not to consent, and withholding consent itself, involves no financial cost to, and little effort from, the individual.[44] In ALRC 96, emphasis was also placed on ensuring that an individual's consent is voluntarily given—that is, not coerced.[45]

- Whether the individual's option to consent to one purpose is freely available and not bundled with other purposes. In ALRC 96, it was stated that 'while the bundling of consents may not be in breach of the *Privacy Act*, the practice has the potential to undermine the voluntariness of the consent of an applicant for insurance'.[46] The ALRC reiterates this view and extends the application beyond the area of insurance contracts to any contractual arrangement. Bundling consent can often be contrary to the spirit of the privacy principles and, in any event, may not be good business practice—especially if it alienates a potential customer.[47] Nevertheless, the ALRC acknowledges that in certain circumstances, particularly where the personal information in question does not fall within the definition of 'sensitive information', it may be appropriate for an agency or organisation to use bundled consent. For example, it can obviate the need to contact a customer repeatedly about minor issues. As explained below, the ALRC proposes that the OPC provide further guidance on the issue of bundled consent and, in particular, when it should not be used.

Options for reform

16.26 There is a need to clarify the issue of consent as it applies to the privacy principles. In order to achieve this goal, there are four principal options for reform. First, the *Privacy Act* and other legislation could set out in detail what is required to obtain the requisite consent in the many contexts in which personal information may be used or disclosed for a secondary purpose. Secondly, the definition of 'consent' in s 6(1) of the *Privacy Act* could be amended to set out with greater precision what factors should be taken into account in obtaining an individual's consent. Thirdly, the OPC could provide more guidance on what constitutes consent for the purposes of the privacy principles in various different contexts. Fourthly, a number of the elements of the above three approaches could be combined.

16.27 The first option for reform would require several, differing statutory definitions of 'consent' to cover the various contexts in which this is an issue. This approach

---

44 See, eg, F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 25.

45 See Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.34]–[28.37].

46 Ibid, [28.46].

47 Ibid, [28.46].

would require a very large number of prescriptive rules that attempt to cover the spectrum of situations in which an agency or organisation may seek consent to use or disclose personal information with the consent of the individual concerned. In relation to the areas covered, this would have the benefit of providing greater regulatory certainty and, in certain situations, it may be appropriate. However, the ALRC's view is that, if applied to all contexts in which personal information is used and disclosed, such an approach would be inconsistent with one of the aims of the *Privacy Act*: to create a regulatory regime that sets out broad, general rules, while minimising fragmentation of privacy law.[48] Moreover, such an approach may be doomed to fail because it would be very difficult, if not impossible, to cover every relevant context.

16.28 The second option is to retain a principles-based approach, but for the Act to state more explicitly, and in greater detail, what is meant by the term 'consent'. As noted above, this would involve amending the current statutory definition of consent.[49] It should be acknowledged that most comparable foreign jurisdictions do not provide a detailed statutory definition of consent in their privacy legislation. There are, however, some examples of statutory definitions of consent. Italian information privacy law contains a provision called 'consent' that states:

> 1. Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent.
>
> 2. The data subject's consent may refer either to the process as a whole or to one or more of the operations thereof.
>
> 3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13.
>
> 4. Consent shall be given in writing of the processing concerns sensitive data.[50]

16.29 A similar definition of consent is provided in German privacy legislation, although it contains more onerous requirements in respect of consent relating to the use of personal information for 'scientific research'.[51]

16.30 The ALRC has given careful consideration to whether the *Privacy Act* should adopt such an approach. Specifically, the ALRC acknowledges that there would be some benefit in adopting a statutory definition of 'consent'. This definition could set out an objective test incorporating a non-exhaustive list of factors that an agency or organisation should point to when arguing that it has obtained the consent of an individual to a particular use or disclosure. Those factors could include those identified above as the four critical elements of consent—namely:

---

48 See, generally, Proposal 15–1 and Part C of this Discussion Paper.

49 The term 'consent' is currently defined to mean 'express consent or implied consent': *Privacy Act 1988* (Cth) s 6(1).

50 *Personal Data Protection Code 2003* (Italy) s 23.

51 *Federal Data Protection Act 1990* (Germany) s 4(a).

- the context in which consent is sought;
- whether there is informed consent;
- whether the consent is voluntary; and
- whether the individual's option to consent to one purpose is freely available and not bundled with other purposes.

16.31 Concern was raised in consultations, however, that a statutory definition of consent along these lines would either not provide substantive assistance in determining whether consent has been given in a particular situation, or it could be interpreted too restrictively, creating an undesirable constriction on the flow of information. It is worth noting that it tends to be civil law jurisdictions that possess a detailed statutory definition of consent. In these jurisdictions, such a process of codification may be more desirable given that there is less scope to develop the law through the process of statutory interpretation by courts and others. It was also suggested that there may be a number of situations where the consent exception, which is currently being relied on to permit use or disclosure, would no longer support a lawful use or disclosure of personal information. The ALRC notes that there has not been strong support for an expanded statutory definition of consent and that such a definition may cause more problems than it solves, particularly if it were to prevent the legitimate handling of personal information by an agency or organisation that has come to rely on the consent exception.

16.32 The third option for reform is for the OPC to provide more guidance on what constitutes consent for the purposes of the privacy principles, particularly for contexts in which there is currently confusion or disagreement as to what is required to obtain an individual's consent. It should be noted that the OPC has already provided some guidance in this area, which states that an organisation will be more likely to show that an individual has consented where:

> • it is likely that the individual received and read the information about the use or disclosure;
>
> • the chance to opt out of the offer is clearly stated and likely to be understood by the individual and the individual is likely to be aware of the implications of not opting out;
>
> • the opting in or opting out is freely available and not bundled with other purposes;
>
> • receiving the chance to opt out involves no financial cost to, and little effort from, the individual;
>
> • opting out involves little effort from, and no or virtually no cost to the individual;
>
> • the consequences of failing to opt out are harmless;

> • if the individual opts out later, the individual is fully restored, where possible and appropriate, to the circumstances they would have been in if they had opted out earlier.[52]

16.33 While this provides some assistance in determining how to approach the issue of consent, the ALRC is of the view that this guidance should be expanded, particularly to cover contentious areas and where there is currently confusion. One such area is bundled consent. Given concerns about when it is and is not appropriate for an agency or organisation to use the mechanism of bundled consent, the ALRC's view is that there would be considerable benefit in OPC guidance on this issue, to provide greater certainty for agencies and organisations and greater protection for individuals.

16.34 The fourth option for reform is to combine the earlier three options. For instance, OPC guidance on the issue of consent could incorporate the critical factors identified above, which are needed to obtain an individual's consent.

16.35 Moreover, if it becomes apparent that the OPC's guidance on this issue is not being heeded or that the consent exceptions in the privacy principles are being relied on inappropriately, then further legislative action may be warranted.[53] For example, if data collectors in a particular field of activity are wrongly claiming to have obtained consent to handle personal information, the ALRC believes that it would be appropriate to enact primary or subordinate legislation to specify what is required to obtain consent in the relevant field of activity.[54] For example, in certain areas—particularly in credit reporting, the telecommunications industry, and health care and research—the applicable subordinate legislation could be amended, if warranted, to provide more detailed rules as to what is required to secure the consent of an individual for the handling of the individual's personal information.

Conclusion

16.36 In conclusion, the ALRC is of the view that the most appropriate reform to deal with the issue of consent under the privacy principles is for the OPC to provide further guidance as to the meaning of consent, explaining how consent may be obtained in certain contexts that are of particular importance—such as, where an individual is entering a financial transaction with an organisation. This guidance should cover consent as it applies in various contexts and it should include advice on when it is and is not appropriate to use the mechanism of bundled consent.

---

52 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 38.

53 Note, also, that the ALRC proposes that the OPC's powers to remedy non-compliance with the privacy principles should be strengthened: see Part F of this Discussion Paper.

54 See, eg, the detailed definition of 'consent' in the context of direct marketing under the *Spam Act 2003* (Cth) sch 2, cl 3.

Proposal 16–1 The Office of the Privacy Commissioner should provide further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should: (a) cover consent as it applies in various contexts; and (b) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

A separate privacy principle dealing with consent?

Background

16.37 As noted above, the IPPs and NPPs already deal with consent—especially in the principles dealing with use and disclosure of personal information. The question addressed in this part of the chapter is whether the proposed UPPs should contain a principle that deals separately with the issue of consent.[55]

16.38 While many jurisdictions do not deal separately with the concept of consent, some—like Canada and Germany[56]—elevate consent to a separate principle or provision. The Canadian *Model Code for the Protection of Personal Information* states:

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[57]

16.39 However, s 7 of the PIPED Act specifies a number of circumstances in which personal information can be collected, used and disclosed without a person's consent or knowledge. The Model Code covers the form of the consent sought by the organisation, the manner in which organisations can seek consent and in which individuals can give consent, as well as the withdrawal of consent by an individual.[58] The United Kingdom's *Data Protection Act 1998* contains provisions setting out how the data protection principles should be interpreted.[59] For example, in relation to the first principle, personal data are not to be processed unless the data subject has given his or her consent to the processing.[60]

16.40 As noted above, the draft Asia-Pacific Privacy Charter also contains a separate consent principle, which states:

> For some Principles, individual consent justifies actions that would otherwise not comply with the Principle. Where consent is relied upon, it must be freely-given,

---

55 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–35.
56 *Federal Data Protection Act 1990* (Germany) s 4a.
57 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principle 4.3.
58 See Ibid sch 1, Principles 4.34, 4.36–4.38.
59 See *Data Protection Act 1998* (UK) sch 1, pt II.
60 Ibid sch 2.

> informed, variable and revocable. Consent is meaningless if people are not given full information, or have no option but to consent in order to obtain a benefit or service.
>
> For Principles where consent normally applies, there are exceptional situations where consent may be insufficient justification.[61]

Submissions and consultations

16.41 There was general opposition to the addition of a discrete privacy principle dealing with consent.[62] There was concern that this could be too onerous if it imposed additional obligations to obtain consent.[63]

16.42 AAMI submitted that, while there is not currently a discrete consent principle, it already 'exists by the very nature of what an organisation needs to do to collect and manage personal information'. Therefore, a separate consent principle would 'add no value'.[64] Moreover, a number of stakeholders submitted that it would be preferable to rely on the consent provisions in the existing privacy principles and to modify those provisions as necessary.[65] It was suggested, for instance, that the consent aspect of the direct marketing provisions should be modified in line with federal legislation aimed at telemarketing and spam.[66]

ALRC's view

16.43 The ALRC notes that the vast majority of stakeholders that commented on this issue were opposed to a separate privacy principle dealing with consent. The ALRC agrees that it would be inappropriate to deal with consent as a discrete privacy principle.

16.44 As explained above, consent is already a critical element of a number of the existing privacy principles—especially those dealing with use and disclosure, transborder data flows and the collection of sensitive information. Although consent is not required for the collection of an individual's non-sensitive personal information, consent is often sought by agencies and organisations in any event.

16.45 In this way, the concept of consent, where appropriate, is built into the architecture of the privacy principles. It seems logical, therefore, to consider the issue

---

61 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, Principle 2.

62 Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; AAMI, *Submission PR 147,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

63 Law Council of Australia, *Submission PR 177,* 8 February 2007.

64 AAMI, *Submission PR 147,* 29 January 2007.

65 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; AAMI, *Submission PR 147,* 29 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

66 AAMI, *Submission PR 147,* 29 January 2007.

of consent as it arises in respect of these aspects of personal information handling, rather than approaching consent as if it were a freestanding principle that operates independently of the various parts of the information cycle.

16.46 Indeed, treating consent as a separate privacy principle may inappropriately elevate consent to being the overriding factor in permitting or restricting the handling of personal information. Professor Fred Cate has stated:

> Requiring choice may be contrary to other activities important to society, such as national security or law enforcement, or to other values, such as freedom of communication. This explains why so many laws that purport to invest individuals with control over information about them exempt so many activities: it simply is not feasible or desirable to provide for individual control …[67]

16.47 Moreover, the ALRC is of the view that the most pressing problem in relation to consent is not its status within other privacy principles, but rather its meaning in the Act and what agencies and organisations should do in order to obtain consent. As explained above, this problem can best be rectified by providing greater guidance as to the meaning of 'consent' and how this applies in particular contexts.

---

67 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 1–2.

17. Anonymity and Pseudonymity

Contents

Introduction 587
Expansion of anonymity principle 588
Expansion of anonymity principle to agencies? 588
The concept of 'pseudonymity' 590
ALRC's view 590
The option to transact anonymously or pseudonymously 593
Submissions and consultations 594
ALRC's view 595
Summary of proposed 'Anonymity and Pseudonymity' principle 597

Introduction

17.1 This chapter concerns the principle of anonymity and pseudonymity. Currently, the *Privacy Act 1988* (Cth) provides a limited right for an individual to transact anonymously with organisations. This right is designed to give individuals, where appropriate, greater control over how much personal information they wish to reveal to organisations with which they transact. Where applicable, it also allows an individual to reveal often intimate, personal information while minimising the risk that this information will be traced back to the individual concerned.

17.2 This chapter focuses on two main issues. The first is whether the anonymity principle should be expanded to cover agencies as well as organisations. Secondly, the chapter considers what should be the content of this principle under the proposed Unified Privacy Principles (UPPs) and, especially, whether the principle should be expanded to cover pseudonymity.

17.3 The Information Privacy Principles (IPPs) do not contain an anonymity principle. On the other hand, the National Privacy Principles (NPPs) provide that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[1]

17.4 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states:

---

1 *Privacy Act 1988* (Cth) sch 3, NPP 8.

> Anonymity is an important dimension of privacy. In some circumstances, it will not be practicable to do business anonymously. In others, there will be legal obligations that require identification of the individual. Unless there is a good practical or legal reason to require identification, organisations should give people the option to operate anonymously. This principle is not intended to facilitate illegal activity.[2]

17.5 NPP 8, the 'Anonymity' principle, complements NPP 1, which prohibits an organisation from collecting information that is not necessary for its functions or activities. In particular, NPP 8 is intended to affect the design of new technologies that collect more information than is necessary when transacting with individuals.[3]

17.6 Some examples of where an individual may wish to transact anonymously with an organisation, and where it may be lawful and practicable to do so, include:

- making a telephone inquiry about a product or service;
- purchasing goods or services from an organisation that employs persons known personally to the individual; and
- using counselling services, especially where information is revealed about a third party.[4]

17.7 Examples of where the law may require an organisation to identify an individual with which it is dealing include where an individual wishes to open a bank account or where reporting requirements are imposed in relation to notifiable diseases.[5]

Expansion of anonymity principle

Expansion of anonymity principle to agencies?

17.8 As noted above, the IPPs do not contain an anonymity principle comparable to NPP 8. Neither is such a provision set out in the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), or in the privacy legislation of some jurisdictions, including New Zealand and the United Kingdom.[6]

17.9 On the other hand, German privacy law imposes obligations in relation to anonymity on both public and private sector bodies.[7] Similarly, Victorian, Tasmanian and Northern Territory privacy laws contain an anonymity principle that is applicable

---

2 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [384].
3 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5510].
4 Ibid, [2–5520].
5 Ibid, [2–5530].
6 See *Privacy Act 1993* (NZ) s 6; *Data Protection Act 1998* (UK) sch 1.
7 See *Federal Data Protection Act 1990* (Germany) s 3a.

to public sector bodies.[8] The question arises whether Australian Government agencies should be subject to an anonymity principle.[9]

Submissions and consultations

17.10 A large number of stakeholders submitted that Commonwealth agencies should be subject to an anonymity principle.[10] The Office of the Privacy Commissioner (OPC) submitted that 'requiring individuals to be identifiable when it is not necessary can serve to limit the choice and control individuals have over their personal information'.[11] The OPC also noted that it could see 'no compelling argument or policy reason for not extending the anonymity principle to agencies'.[12]

17.11 The Australian Government Department of Health and Ageing supported extending the anonymity principle to government agencies, provided that the principle is framed so as not to interfere unreasonably with an agency's accountability obligations.[13] One stakeholder expressed concern that an extended anonymity principle should not interfere with important functions of particular agencies. For example, such a principle could interfere with a school's duty of care, if it permitted parents of pupils to withhold, say, their home contact information.[14] Balanced against these concerns, however, it should be noted that the requirements in the anonymity principle are qualified, in the sense that they only apply to the extent that it is 'lawful and practicable'. There are likely to be many instances where these qualifications will operate to permit the agency to require individuals to identify themselves.[15]

17.12 Other stakeholders simply opposed, without detailed explanation, any extension of the anonymity principle to agencies.[16] The Australian Taxation Office submitted that a general principle would be inappropriate because:

> While it is possible for individuals to remain anonymous for some interactions, it would not be appropriate to provide a right to deal with regulatory agencies without

---

8 *Information Privacy Act 2000* (Vic) sch 1, IPP 8.1; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 8; *Information Act 2002* (NT) sch 2, IPP 8.

9 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–30.

10 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

11 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

12 Ibid.

13 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

14 Confidential, *Submission PR 130,* 17 January 2007.

15 This point was highlighted in some submissions, including: Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

16 Confidential, *Submission PR 165,* 1 February 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

> identifying themselves. To correctly apply the law the Tax Office needs to know who it is dealing with and must be able to contact people in order to ensure they have met their obligations.[17]

The concept of 'pseudonymity'

17.13 There is a question whether the concept of anonymity is too limited and, in particular, whether the relevant privacy principle should be expanded specifically to include the concept of pseudonymity. If so, this would allow an individual to transact, subject to the relevant qualifications, pseudonymously with a data collector. That would usually involve the individual providing the data collector with some name, term or other combination of letters and/or numerals. Therefore, the individual may select a pseudonym that bears no relation to the individual's actual name, as occurs commonly with internet usernames. In this way, the data collector is able to address the individual specifically and to correspond with the individual without the individual being required to provide the data collector with his or her name or other identifying information.

17.14 A number of stakeholders submitted that the anonymity principle should be extended to make provision for individuals to transact with an agency or organisation pseudonymously, as well as anonymously, where appropriate.[18] For instance, it was submitted that the principle should 'impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties'.[19]

17.15 There is an example of this approach in the *Federal Data Protection Act 1990* (Germany), which contains a provision that deals with pseudonymisation. The term 'pseudonymisation' is defined as 'the replacement of the name and other identifying attributes with a code with a view to making it impossible or significantly more difficult to identify the data subject'.[20] In other words, the German provision differs from the IPPs and NPPs by including the additional concept of psuedonymisation, and imposes these obligations on public bodies.

ALRC's view

Expansion of anonymity principle to agencies?

17.16 A significant majority of stakeholders that commented on this issue favoured extending the principle dealing with anonymity so that it applies to agencies, in addition to organisations (which are already covered by NPP 8). Provided the resulting

---

17 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

18 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

19 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

20 *Federal Data Protection Act 1990* (Germany) s 3(6a).

privacy principle is appropriately worded, the ALRC is of the view that such an extension is desirable for a number of reasons.

17.17 First, giving an individual the option to transact anonymously, where appropriate, allows the individual to retain greater control over their privacy. There are also strong policy reasons to provide this option. For example, this option might encourage an individual (such as a person under the age of 18) to seek medical or other assistance from an agency in circumstances where, if the assistance was contingent on the individual identifying himself or herself, it would discourage the individual from seeking the assistance at all. Secondly, as the OPC stated, there seems no sound policy reason to limit the application of this principle to organisations, particularly given that other jurisdictions contain an anonymity principle that is applicable also to government bodies.

17.18 The ALRC proposes retaining the important qualifications of lawfulness and practicability, which are currently in NPP 8. The ALRC believes that they are appropriate limitations on an individual's right to transact anonymously or pseudonymously (as discussed below). That is, an agency or organisation would not be under an obligation to give the option to an individual to transact anonymously or pseudonymously if, in doing so, this would result in any of the following outcomes:

- the failure to collect the identifying information by the agency or organisation would itself be unlawful. For example, it would be unlawful if the agency or organisation would be unable to comply with a law requiring it to notify a law enforcement body of the transaction in question or to carry out its accountability obligations;

- the failure to collect the identifying information by the agency or organisation would result in the individual acting unlawfully. An example of this is where an individual wishes to transact anonymously to further a fraudulent conspiracy of which the individual is a part; or

- it would be impracticable for the agency or organisation. For example, it may place an unreasonable financial burden on its ability to provide a service to the individual.

17.19 To the extent that these qualifications are not already clear from the natural and ordinary meaning of the words of the relevant privacy principle, the ALRC believes that the OPC should provide guidance to assist agencies and organisations in discerning when it is and is not lawful and practicable to give individuals the option of transacting anonymously or pseudonymously.[21]

---

21 The ALRC's proposal to this effect is located at the end of this chapter.

The concept of 'pseudonymity'

17.20 The ALRC is of the view that the proposed UPPs should enable, where appropriate, an individual to transact pseudonymously, as well as anonymously, with an agency or organisation. Such a provision is particularly useful in the online environment. Often it is necessary for an agency or organisation that runs a website to have *some* means of differentiating between individuals but this does not necessarily mean the agency or organisation needs to know an individual's name or other identifying personal details. For instance, websites often require a 'username' and password for this purpose. Whether an individual chooses, as a username, his or her actual name or whether the individual chooses some other form of letters and/or numbers will often be immaterial to the agency or organisation. The ALRC believes that, subject to the qualifications of practicability and lawfulness, the privacy principles should reflect this.

17.21 The ALRC also believes that if the proposed UPPs provide an option for an individual to interact pseudonymously, it would allow the principle to operate more flexibly. This is because it would cover the situation, not currently dealt with explicitly by NPP 8, where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation. Furthermore, an extension of the principle to encompass pseudonymous transactions would encourage agencies and organisations to incorporate into their systems privacy enhancing technologies that facilitate pseudonymous interactions in an online environment.[22]

17.22 Finally, the ALRC believes that any extension of the principle to cover pseudonymous transactions would need to be worded carefully to minimise the risk of fraud or misleading practices. The ALRC is of the view that the situation of fraud is likely to be covered effectively by the qualifications already in NPP 8. The fact that organisations are only required to provide the option to transact anonymously (or pseudonymously, as proposed here) where it would be 'lawful and practicable' would mean that an organisation is not required to provide this option where there is a real risk of fraud.

17.23 However, it may nevertheless be misleading, even where not necessarily fraudulent, for an individual to provide a pseudonym—or particular types of pseudonym—in some circumstances. For example, it is likely to be misleading for an individual deliberately to choose, as a pseudonym, someone else's name in order to give the impression that he or she is actually that other person. Consequently, the ALRC proposes that the option to transact pseudonymously should be subject to a further limitation that does not apply to the right to transact anonymously—that is, it should be limited to situations where it would not be misleading.

---

22 See the detailed discussion on privacy and developing technology in Part B.

Application of the principle

17.24 One small, miscellaneous matter that was raised in submissions and consultations was over the wording of this privacy principle. Currently, NPP 8 requires organisations to provide the option of anonymity to individuals 'when entering transactions with an organisation'. The OPC submitted that this should be amended to make clear that where 'an individual has an existing relationship with an organisation, that individual is still entitled to transact anonymously', subject to the other relevant qualifications.[23]

17.25 The ALRC agrees that this clarification should be incorporated into the 'Anonymity and Pseudonymity' principle in the proposed UPPs. This can be achieved by replacing the words 'when entering transactions' in the current NPP 8 with the words 'when transacting'.

Proposal 17–1 The proposed Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that sets out the requirements on agencies and organisations in respect of anonymous and pseudonymous transactions with individuals.

Proposal 17–2 The proposed 'Anonymity and Pseudonymity' principle should include a pseudonymity requirement that when an individual is transacting with an agency or organisation, the agency or organisation must give the individual the option of identifying himself or herself by a pseudonym. This requirement is limited to circumstances where providing this option is lawful, practicable and not misleading.

The option to transact anonymously or pseudonymously

17.26 As explained above, the ALRC proposes that agencies and organisations should only be required to provide the option to transact anonymously where two conditions are fulfilled: it must be 'lawful', and it must be 'practicable'.[24] The ALRC proposes an additional condition in respect of pseudonymous transactions—namely, that it is 'not misleading'. Where these conditions are satisfied, the following question arises: what should an agency or organisation do to ensure that individuals have the option to transact anonymously or pseudonymously?

17.27 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the anonymity privacy principle should expressly require organisations to give

23 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
24 This reflects the conditions in *Privacy Act 1988* (Cth) sch 3, NPP 8.

an individual the option of remaining anonymous when entering into transactions with the data collector.[25] In other words, the ALRC solicited views on whether agencies or organisations should be required to ask individuals expressly whether they wish to transact anonymously or pseudonymously.

17.28 It should be noted, for example, that the wording of the Northern Territory's anonymity principle differs from that of NPP 8, in that it expressly identifies the obligation imposed on a data collector:

> A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.[26]

Submissions and consultations

17.29 A number of stakeholders supported amending the relevant privacy principle to impose a 'positive obligation' on agencies and organisations 'to ensure that the individual is provided with the choice as to whether or not to interact anonymously'.[27] The OPC submitted that this requirement would be beneficial because it would encourage agencies and organisations to consider 'whether they need to identify the individual (and thus collect their personal information) for each and every transaction'.[28] The Australian Privacy Foundation, and others, submitted that this is consistent with the 'touchstone' in this area—namely, that an entity should engage in only the 'minimum collection necessary for the purpose of the transaction'.[29] Assuming that the existing qualifications in NPP 8 are retained, AAMI supported a requirement on organisations to give individuals the *specific* option of remaining anonymous.[30]

17.30 Other stakeholders opposed the imposition of a requirement to give individuals the express option of remaining anonymous when entering into transactions with the data collector.[31] The Law Council of Australia argued that the requirement in NPP 1 that an organisation only collect relevant information provided sufficient protection for

---

25 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–29. This Question was phrased with reference to organisations, as distinct from agencies, given that under the current *Privacy Act* only organisations are subject to an anonymity principle.

26 *Information Act 2002* (NT) sch 2, IPP 8.

27 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007.

28 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

29 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; K Pospisek, *Submission PR 104,* 15 January 2007.

30 AAMI, *Submission PR 147,* 29 January 2007.

31 Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

individuals.[32] AXA submitted that this would 'create unnecessary disputes about whether a particular transaction is one to which the right to anonymity applies'.[33] The National Australia Bank and MLC submitted that such a requirement would be unworkable for financial institutions.[34] Others were concerned that it would encourage 'fraud'[35] or be open to 'abuse'.[36] Similarly, the Australian Federal Police feared that any broadening of the anonymity principle could 'be exploited by individuals to commit crimes'.[37]

17.31 Some refinements to the content of the anonymity principle were also suggested. For example, it was submitted that the principle should be clarified to apply 'at the stage when an information system is being designed, not only "after the event" when a person wishes to enter a transaction with a data user'.[38] Another stakeholder argued that the principle should be structured so it is easier to apply 'in the modern computer age'.[39]

ALRC's view

17.32 The ALRC believes that it is preferable to require data collectors to give individuals the clear option of transacting anonymously or pseudonymously. It is first necessary to distinguish between an obligation to provide an *express* option to individuals and an obligation to provide a *clear* option. An express option would require a data collector to state explicitly that individuals may transact anonymously or pseudonymously. A clear option, however, is less prescriptive and merely requires that the data collector ensure that individuals are aware that they may transact anonymously or pseudonymously. As explained below, a requirement to provide individuals with a clear option would be less onerous and cumbersome, in most instances, than a requirement to provide an express option because it would allow agencies and organisations to comply with the proposed Anonymity and Pseudonymity principle in the *structure* of their information collecting systems.

17.33 In formulating this proposal, the ALRC has sought to balance competing considerations. On one hand, expressly inviting individuals to transact anonymously or pseudonymously—that is, what is referred to above as providing 'an express option'—would emphasise to individuals their right to withhold some of their personal information in certain transactions. As noted by stakeholders, it would also encourage

---

32 Law Council of Australia, *Submission PR 177,* 8 February 2007.
33 AXA, *Submission PR 119,* 15 January 2007. See also Law Council of Australia, *Submission PR 177,* 8 February 2007.
34 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.
35 Telstra, *Submission PR 185,* 9 February 2007.
36 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
37 Australian Federal Police, *Submission PR 186,* 9 February 2007.
38 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
39 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

agencies and organisations to design their information-collecting systems so as not to intrude unnecessarily on individuals' privacy. However, provided the option to transact anonymously or pseudonymously is clearly available, the ALRC believes that this goal will be achieved without necessarily asking individuals explicitly whether they wish to transact anonymously or pseudonymously.

17.34 A number of stakeholders stressed that a requirement to provide an express option, on some interpretations, could be quite onerous. For this reason, the ALRC proposes that the OPC should issue guidance clarifying what is involved in providing a clear option to transact anonymously or pseudonymously. For example, in many cases where asked to fill out a form either on paper or electronically, individuals are told which fields they must complete.[40] It would not be overly burdensome to alter the list of 'required fields' to take account of the proposed Anonymity and Pseudonymity principle. In the ALRC's view, this would provide an individual with a clear option to transact anonymously or pseudonymously without imposing unreasonable demands on the agency or organisation to alter radically its information-collecting systems.

17.35 Moreover, the requirement would remain subject to the 'practicability' qualification. This qualification allows an agency or organisation not to provide the option to transact anonymously or pseudonymously if the resulting change to its systems would cause unjustifiable hardship.

17.36 Finally, as explained above, this requirement would remain subject to the qualifications of lawfulness and practicability and, in the case of pseudonymous transactions, the additional 'not misleading' qualification. The ALRC believes that these would be sufficient to make sure that the option does not encourage fraud or other types of unlawful activity.

Proposal 17–3 The proposed 'Anonymity and Pseudonymity' principle should provide that, subject to the relevant qualifications in the principle, an agency or organisation is required to give individuals the clear option to transact anonymously or pseudonymously.

Proposal 17–4 The Office of the Privacy Commissioner should provide guidance to agencies and organisations on: (a) when it is and is not lawful and practicable to give individuals the option to transact anonymously or pseudonymously; (b) when it would be misleading for an individual to transact pseudonymously with an agency or organisation; and (c) what is involved in providing a clear option to transact anonymously or pseudonymously.

40 A 'field', on a form, is the space reserved for an individual to provide his or her response to a question that is asked on the form.

Summary of proposed 'Anonymity and Pseudonymity' principle

17.37 In summary, the ALRC's view is that the first principle in the proposed UPPs should be called 'Anonymity and Pseudonymity'. It should appear as follows.

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable, individuals, when transacting with an agency or organisation, should have the clear option of either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym, provided this would not be misleading.

18. Collection

Contents

Introduction 599
Current coverage by IPPs and NPPs 600
Collection from the individual 601
Background 601
Submissions and consultations 602
ALRC's view 603
Unsolicited personal information 605
Background 605
Submissions and consultations 605
ALRC's view 607
Other aspects of the 'Collection' principle 608
Location of notification requirements 608
Collection of sensitive information 608
Limitation on collection: reasonable purposes? 609
Summary of proposed 'Collection' principle 610

Introduction

18.1 The privacy principles in the *Privacy Act 1988* (Cth) contain limitations on what personal information may lawfully be collected. Significantly, neither the Information Privacy Principles (IPPs) nor the National Privacy Principles (NPPs) require that an individual give his or her consent before an agency or organisation is permitted to collect the individual's personal information.[1] The current limitations on the collection of personal information are set out below.

18.2 This chapter considers the limitations that should apply to agencies and organisations that wish to collect personal information. It also analyses what is meant by the term 'collection' and, in particular, how the proposed Unified Privacy Principles (UPPs) should deal with unsolicited personal information that is received by agencies and organisations.

---

1 Note, however, that there is a general prohibition, subject to a finite list of exceptions, against the collection of sensitive information by organisations. One of these exceptions is where the individual consents to the collection. See Ch 19.

Current coverage by IPPs and NPPs

18.3 IPPs 1–3 deal with the collection of personal information by government agencies. IPP 1 provides that personal information shall not be collected for inclusion in a 'record' or in a 'generally available publication' unless: (a) the purpose for which the information is collected is lawful and directly related to a function or activity of the collector, and (b) the collection of the information is necessary for or directly related to that purpose. The Privacy Commissioner has expressed the view that 'purpose of collection' is to be interpreted narrowly, and that agencies should have a clear purpose for collecting each piece of personal information. It is not generally acceptable for an agency to collect information just because it may be useful in the future.[2] In addition, personal information is not to be collected by unlawful or unfair means.

18.4 IPPs 2 and 3 cover 'solicitation' of personal information. IPP 2 provides that where an agency solicits personal information directly from the individual concerned for inclusion in a record or a generally available publication, the agency must take reasonable steps to ensure that, before or soon after the information is collected, the individual is generally aware of:

- the purpose for which the information is being collected;
- if the collection is authorised or required by law—that fact; and
- to whom it is the agency's usual practice to disclose or pass on personal information of the kind collected.

18.5 The Explanatory Memorandum notes that there would be circumstances in which an agency would not need to take any steps to ensure that the individual was aware of the matters specified in IPP 2 when soliciting personal information from that person.[3]

18.6 IPP 3 provides that where an agency solicits personal information for inclusion in a record or in a generally available publication, it must take reasonable steps, having regard to the purpose for which the information is collected, to ensure that:

- the information is relevant to that purpose, up-to-date and complete; and
- the collection does not intrude unreasonably on the individual's personal affairs.

---

2 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994).

3 See Explanatory Memorandum, Privacy Bill 1988 (Cth), [61].

18.7 This principle is limited to personal information solicited from the individual and from third parties. It does not extend to information received without solicitation by the agency.[4]

18.8 NPP 1 provides that an organisation[5] may only collect personal information:

- that is necessary for one or more of its functions or activities;
- by lawful and fair means and not in an unreasonably intrusive manner;
- after taking reasonable steps to ensure the individual is aware of: the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; the organisations to whom the organisation usually discloses information of that kind; any law requiring the particular information to be collected; and the main consequences for the individual if the information is not provided; and
- from that individual if it is reasonable and practicable to do so, or from someone else if it takes reasonable steps to ensure that the individual is aware of the matters listed above, except to the extent that making the individual aware would pose a serious threat to anyone's life or health.

18.9 Special rules apply to the collection of sensitive information in NPP 10. 'Sensitive information', which is defined in s 6(1) of the Act, is a subset of 'personal information', and it is dealt with separately in Chapter 19.

Collection from the individual

Background

18.10 NPP 1 obliges an organisation, where reasonable and practicable, to collect personal information about an individual *only* from that individual. IPPs 1–3 impose no equivalent requirement on agencies. In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether this lacuna that applies to agencies should be closed.[6]

18.11 It should be noted that some other jurisdictions require public sector bodies, where reasonable, only to collect personal information from the individual concerned. In New South Wales, such an obligation applies to public sector agencies unless the individual concerned has authorised collection from someone else or, where the information relates to a person under 16 years, the information has been provided by a

4 Ibid, [63].
5 'Organisation' is defined in *Privacy Act 1988* (Cth) s 6C. The definition is discussed in Ch 3.
6 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–3.

parent or guardian.[7] Privacy laws in Canada, New Zealand and Germany all require a government institution, where possible, to collect personal information that it intends to use for an administrative purpose directly from the individual to whom it relates except in certain specified circumstances.[8] Similarly, US law requires agencies to

> collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.[9]

Submissions and consultations

18.12 A large number of stakeholders responding to this question argued that there was no reason to retain different rules for agencies and organisations in these circumstances.[10] There were, however, some who took the opposite view, arguing that there should not be a general requirement on agencies to collect personal information about an individual from the individual in question.[11]

18.13 One submission argued that two general benefits would flow from extending the requirement to agencies that, where reasonable and practicable, information about an individual should only be collected from that individual:

> This requirement contributes to the fairness and transparency of processing personal data by helping to ensure that the data subjects participate in that processing. The requirement may also promote accuracy, relevance etc of personal data.[12]

18.14 It was stated that this requirement should be based on NPP 1.4, but that the word 'only' in that provision should be deleted to accommodate collection from both an individual and a third party (where justified).[13]

18.15 A number of stakeholders expressed qualified support for a general requirement on agencies to collect personal information about an individual only from the

---

7 *Privacy and Personal Information Protection Act 1998* (NSW) s 9.

8 See *Privacy Act* RS 1985, c P-21 (Canada) s 5(1); *Privacy Act 1993* (NZ) s 6, IPP 2; *Federal Data Protection Act 1990* (Germany) s 4(2).

9 See *Privacy Act 1974* 5 USC § 552a (US).

10 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

11 Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; Confidential, *Submission PR 165,* 1 February 2007.

12 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

13 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

individual in question. Some emphasised that such a requirement should only apply where 'reasonable and practicable' and that collection should not be jeopardised when it is not reasonable or practicable to obtain the information from the individual.[14] The Australian Government Department of Human Services pointed out that it is sometimes necessary to collect personal information from third parties 'to prevent or lessen the instances of fraud and ensure the protection of public monies'.[15] Similarly, the Australian Competition and Consumer Commission (ACCC) submitted that it would deter people from making complaints and hamper the ACCC's investigations, if it were deemed reasonable and practical for the ACCC to seek customer details relating to one of its investigations only from the customer in question.[16]

18.16 Some stakeholders opposed any change. The Australian Federal Police (AFP) argued that law enforcement agencies routinely collect personal information from a range of sources, and that a 'reasonable and practicable test may not be sensitive enough to recognise this and may have significant operational impacts'.[17] The Australian Taxation Office made a similar point, arguing that while agencies should be encouraged to liaise with the individual about whom they are seeking personal information, it should not be 'mandatory' to do so.[18] The Australian Government Department of Families, Community Services and Indigenous Affairs (FaCSIA) submitted that such a requirement would hamper agencies' whole of government approach to service delivery because:

> Requiring each agency to separately collect information from the individual for the same programme would lead to a duplication of process and increase administrative inefficiency of government agencies.[19]

ALRC's view

18.17 In the ALRC's view, agencies and organisations should both be required, where reasonable and practicable, to collect personal information about an individual only from the individual concerned. As noted above, this requirement already applies to organisations; the ALRC proposes to extend the requirement to include agencies as well. Such an amendment would also bring agencies in line with similar requirements

---

14 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

15 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

16 Australian Competition and Consumer Commission, *Submission PR 178,* 31 January 2007.

17 Australian Federal Police, *Submission PR 186,* 9 February 2007. See also Confidential, *Submission PR 165,* 1 February 2007.

18 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

19 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

in other jurisdictions within Australia and overseas. The ALRC observes that this reform received full or qualified support from the overwhelming majority of stakeholders that commented on this issue, including from a number of agencies, organisations and other entities.

18.18 One important qualification is that this requirement would only apply 'where reasonable and practicable'. This qualification is significant, particularly as it applies to agencies. Agencies—especially those that are empowered by law to obtain personal information coercively—would be able to exercise this qualification more readily than many organisations, which are less likely to be subject to such a law. This is an intended consequence, and one that should assuage some concerns expressed by agencies that such a reform could hamper their ability to perform their statutory duties.

18.19 Finally, the ALRC believes that there should be further guidance to clarify when it would *not* be reasonable and practicable to collect personal information from the individual concerned. Such guidance could be provided either in the *Privacy Act* itself or by the Office of the Privacy Commissioner (OPC). The first option would involve amending the collection principle, or some other provision in the Act, to set out a list of factors to take into account in determining whether it is reasonable and practicable to collect personal information from the individual concerned.

18.20 The second option would involve the OPC working with agencies and organisations to assist them in understanding when this requirement would be triggered, and when they need not collect personal information from the individual concerned. The ALRC prefers the second option—that the OPC provide guidance on this issue—because an amendment to the Act would be more prescriptive and rigid, and it would also conflict with the general aim to adopt principles as the main mode of privacy regulation.[20]

Proposal 18–1 (a) The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

(b) The Office of the Privacy Commissioner should provide guidance to clarify when it would not be reasonable and practicable to collect such information from the individual concerned.

20 See Proposal 15–1 and accompanying text in Ch 15.

Unsolicited personal information

Background

18.21 Agencies and organisations sometimes receive unsolicited personal information. This occurs where personal information about an individual is received by an agency or organisation that has taken no active steps to collect that information. Differing obligations apply as between the IPPs and NPPs in respect of unsolicited information.

18.22 Where an agency receives unsolicited material—from sources such as a Ministerial letter or a tip-off from an informer—it must comply with IPP 1.[21] Sometimes unsolicited personal information received by an agency is particularly sensitive—for instance, in the area of community services, it may receive information relating to domestic violence or abuse. It has been noted that where such information remains on file, 'there is a danger that it will indirectly influence an agency official in their decisions about, or interactions with, the individual'.[22]

18.23 In contrast, the NPPs do not explicitly distinguish between the obligations on an organisation in respect of solicited and unsolicited information. As noted above, however, NPP 1 does separately address personal information obtained directly from the individual concerned, and information collected from 'someone else'.[23]

18.24 The ALRC asked in IP 31 what obligations, if any, should apply to an agency or organisation where it receives unsolicited information that it intends to include in a record or a generally available publication.[24]

Submissions and consultations

18.25 A number of stakeholders stated that, where an agency or organisation receives unsolicited personal information, this information should be covered by the privacy principles.[25] Some stakeholders suggested specific obligations that should apply in respect of unsolicited information:

- The 'accuracy of such information should be checked as soon as possible with the subject, where possible, unless the source is a publicly available source'.[26]

---

21 See Explanatory Memorandum, Privacy Bill 1988 (Cth), [59].

22 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

23 See *Privacy Act 1988* (Cth) sch 3, NPPs 1.4, 1.5.

24 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–4.

25 See, eg, G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

26 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A number of other stakeholders expressed similar views: see, eg, Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

The OPC submitted that this was particularly important where the information may be used to deny an individual 'access to essential services'.[27]

- The individual should be given the opportunity to consent (or refuse) to his or her personal information being used in these circumstances.[28] One stakeholder argued that this would assist in achieving the purpose and object of the *Privacy Act*.[29]

- Unsolicited information that is 'irrelevant to the functions' of the entity that receives it should be destroyed.[30]

18.26 Others stated that such an obligation should not be imposed because the existing rules are sufficient in respect of unsolicited information.[31] For example, the Centre for Law and Genetics argued that the distinction between solicited and unsolicited information derives from paper-based record keeping and 'should not be maintained in a modern computer-data driven environment'. Therefore, where an organisation or agency proposes to keep or use unsolicited information, it should be subject to the usual privacy principles.[32]

18.27 Some stakeholders submitted that if obligations, such as those in NPP 1.3 and 1.5, were applied to all unsolicited information, it 'would impose a significant administrative burden on organisations'.[33] It is, therefore, necessary to distinguish between unsolicited information that is merely *received* and where it is actually *retained*, and that obligations should only apply where the information is retained by the organisation.[34]

18.28 It was also argued that such an obligation should not apply in respect of alternative dispute resolution (ADR) schemes.[35] The question whether such schemes

---

27 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

28 I Turnbull, *Submission PR 82,* 12 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

29 I Turnbull, *Submission PR 82,* 12 January 2007.

30 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. A similar point was raised by Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

31 See, eg, Australian Federal Police, *Submission PR 186,* 9 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Confidential, *Submission PR 143,* 24 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

32 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007. A similar point was made in respect of unsolicited health information: National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

33 DLA Phillips Fox, *Submission PR 111,* 15 January 2007. See also Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

34 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

35 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007.

should be exempted from the operation of this and any other privacy principles is dealt with in Part E.

ALRC's view

18.29 The ALRC recognises that many agencies and organisations receive a large amount of unsolicited personal information. This is heightened in the digital age where information can be transmitted easily and quickly, sometimes in circumstances where the entity disclosing the information does not consider whether it falls within the definition of personal information.

18.30 In the ALRC's view, the fact that an agency or organisation has done nothing to cause personal information to be sent to it should not mean that such information falls outside the protection of the privacy principles. Indeed, as noted above, the current IPPs and NPPs already impose obligations in respect of unsolicited personal information. The main question is: what should those obligations be?

18.31 The ALRC acknowledges that it would be onerous to require organisations and agencies to comply, in respect of all unsolicited personal information that they receive, with all obligations under the IPPs and NPPs, when they have taken no active steps to collect it. For example, the cost of complying with the specific notification requirements alone could be significant.

18.32 The risk that personal information will be used or disclosed in violation of a person's right to privacy only becomes significant where, on receiving unsolicited personal information, the entity decides to retain it. Consequently, by making it clear that the collection principle applies where an entity collects *or* retains personal information that it has received from a third party, this will require the entity to consider whether it:

- can lawfully collect such information and, if so,
- wishes to retain such information.

18.33 If the answer to either of these questions is 'no', the entity should immediately destroy the information in question without using or disclosing it. If the answer to both of the above questions is 'yes', then the usual requirements with respect to personal information that is 'actively' collected should apply. Unless an exception applies, this would involve informing the individual concerned, for example, that the collection has taken place, that he or she may access the information to check its accuracy and so on. It would also mean that the spectrum of personal information that an agency or organisation may lawfully retain, use and disclose is not expanded merely because the entity has taken no steps to collect the information. This is because the threshold requirements—including that an agency or organisation is only permitted to collect

personal information that is 'necessary for one or more of its functions or activities'—would continue to apply if it wishes to retain the information after it has received it.

Proposal 18–2 The 'Collection' principle in the proposed UPPs should provide that, where an agency or organisation receives unsolicited personal information, it must either: (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

Other aspects of the 'Collection' principle

Location of notification requirements

18.34 As noted above, the collection principles in both the NPPs and IPPs provide that, in certain circumstances, agencies and organisations must notify an individual whose personal information has been, or is to be collected, of a number of matters. A question arises as to whether the proposed 'Collection' principle of the UPPs should set out the notification requirements that apply at or around the time the information is collected, or whether these requirements should be set out in another principle that relates more explicitly to notification.

18.35 This issue is dealt with in Chapter 20, where the ALRC proposes that the notification requirements that are currently located in the collection principles in the IPPs and NPPs should be moved to a separate privacy principle called 'Specific Notification'.[36]

Collection of sensitive information

18.36 Currently, the collection of sensitive information by organisations is covered in a separate privacy principle, NPP 10. Conversely, the collection of sensitive information by agencies is not dealt with explicitly in the IPPs.

18.37 A question arises as to whether the proposed 'Collection' principle in the UPPs should also deal with the collection of sensitive information, or whether sensitive information should continue to be dealt with separately. This question is addressed in Chapter 19, where the ALRC proposes that the provisions that relate to the collection of sensitive information should be contained in the 'Collection' principle.[37]

36 See Proposals 20–1 and 20–2.
37 See Proposal 19–1.

Limitation on collection: reasonable purposes?

18.38 A question arises as to whether the proposed 'Collection' principle in the UPPs should limit the ability of agencies and organisations to collect personal information to purposes that a reasonable person would consider appropriate in the circumstances. This would make clear it that an objective test applies in assessing what is an agency's or organisation's purpose in collecting personal information.

18.39 The Australian Privacy Foundation submitted to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry) that the NPPs should provide that collection should be limited by such an objective test.[38] The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) rejected the adoption of an objective test to ascertain whether collection of personal information was necessary for an organisation's functions or activities. It stated that, while it would enable an individual to challenge the collection of personal information, it would be difficult to implement in practice and 'it is not likely that the benefits of doing so would outweigh the costs'.[39]

18.40 In its submission to this Inquiry, however, the OPC seems to have changed its position, suggesting that the collection principle 'could include' a requirement that 'the collection would be considered necessary and legitimate by a reasonable person'.[40] It went on to state:

> The legitimacy of collection might be strengthened by the introduction of a 'reasonable person test' to the collection principle … Such a measure may reduce the degree to which organisations employ advanced technologies to collect personal information for functions that may not ordinarily be considered legitimate when approached objectively.[41]

18.41 By way of comparison, some Canadian privacy law provides for an objective test in these circumstances. For instance, the federal legislation provides that an organisation may collect, use or disclose personal information 'only for purposes that a reasonable person would consider are appropriate in the circumstances'.[42] Similarly, Alberta's information privacy legislation states:

---

38 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.170]. See also Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

39 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

40 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

41 Ibid.

42 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 5(3). See also s 3.

> Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.[43]

ALRC's view

18.42 The ALRC's view is that it would be desirable—largely to reduce any existing ambiguity—to amend this aspect of the collection principle, by making clear that it is necessary to consider objectively (rather than subjectively) what is 'necessary' for an agency's or organisation's functions or activities. There is a strong argument that this is already implicit in the existing NPP 1 and, in any event, it is certainly within the spirit of the privacy principles as a whole.

18.43 The benefit of such an amendment is that it would provide greater clarity where an agency or organisation claims to be collecting an individual's personal information for the legitimate purpose of providing a service to the individual, but where it is clear that the agency's or organisation's *real* purpose is an illegitimate one, like on-selling the data to a third party. In this situation, the collection principle would make it plain that the data collector cannot simply point to its subjective view as to its purpose; rather it would focus analysis onto what a reasonable person in the position of the agency or organisation would believe to be the agency's or organisation's purpose.

18.44 A further benefit of this proposed amendment is that it would create greater incentive for agencies and organisations to consider the potential impact of any new data collection prior to the collection itself. For example, where an organisation uses a biometrics system for the purposes of data collection, an objective test would encourage the organisation to give more careful consideration to whether the personal information it collects is genuinely necessary for its functions.

Proposal 18–3 The 'Collection' principle in the proposed UPPs should provide that an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.

Summary of proposed 'Collection' principle

18.45 In summary, the ALRC's view is that the second principle in the proposed UPPs should be called 'Collection'. It should appear as follows.

---

43 *Personal Information Protection Act 2003* RS (Alberta) c.P–6.5 s 11(2). In IP 31, the ALRC sought views on whether a similar test should be introduced in the *Privacy Act*: See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.68], [11.127]. This issue, however, was not addressed in submissions and consultations, other than by the OPC.

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation collects personal information about an individual from the individual or from someone else, it must comply with UPP 3.

2.5 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

(a) destroy the information immediately without using or disclosing it; or

(b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.6 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required or specifically authorised by or under law; or

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent; or

(d) if the information is collected in the course of the activities of a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

19. Sensitive Information

Contents

Introduction 613
Background 613
Current coverage by IPPs and NPPs 614
Expansion of sensitive information principle to agencies? 615
Background 615
Submissions and consultations 616
ALRC's view 616
Regulation of other aspects of sensitive information handling 618
Background 618
Submissions and consultations 619
ALRC's view 620
Emergency situations 622
ALRC's view 622
Emergency situations not involving a serious threat to life or health 623
Research 625

Introduction

Background

19.1 This chapter concerns the collection of sensitive information. The *Privacy Act 1988* (Cth) distinguishes between 'personal information' and 'sensitive information'. Both terms are defined in s 6(1) of the *Privacy Act*, and these definitions are discussed in Chapter 3. Essentially, however, sensitive information is a subset of personal information. The National Privacy Principles (NPPs) provide additional restrictions on the collection of sensitive information by private sector organisations. However, the Information Privacy Principles (IPPs), which apply to government agencies, contain no equivalent restriction.

19.2 There is considerable, although not universal, international support for treating sensitive information separately. A number of other jurisdictions, such as Canada, provide for additional privacy protections in respect of sensitive information.[1] Moreover, the European Parliament's *Directive on the Protection of Individuals with*

1 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, cl 4.3.

Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995) (EU Directive) provides that member states should impose additional restrictions on the processing of sensitive personal information.[2] A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under art 29 of the EU Directive, highlighted the importance of providing additional protection to sensitive information, by stating that

> where 'sensitive' categories of data are involved … additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.[3]

19.3 This chapter focuses on two main issues. The first is whether the privacy principle dealing with sensitive information should be expanded to cover agencies as well as organisations. This question has particular significance if the ALRC's proposal to move to the Unified Privacy Principles (UPPs) is adopted.[4] Secondly, the chapter considers whether the *Privacy Act* should regulate other aspects of the handling of sensitive information in addition to collection. This could include the use, disclosure, storage, access, retention and disposal of sensitive information.

Current coverage by IPPs and NPPs

19.4 As noted above, the IPPs do not regulate the collection of sensitive information separately from other forms of personal information. Conversely, NPP 10 prohibits the collection of sensitive information, except in certain identified circumstances. NPP 10.1 provides that sensitive information can be collected only if:

- the individual has consented;
- the collection is required by law;[5]
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of an individual and the individual is physically or legally incapable of giving or communicating consent to the collection; or
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

---

2 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 8.

3 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998.

4 See Proposal 15–2.

5 There is no general exception in NPP 10.1 where the collection is merely authorised, but not required, by law.

19.5 In addition, NPP 10.1 allows sensitive information to be collected in the course of the activities of a non-profit organisation.[6] This is permitted where: (a) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and (b) at or before the time of collection, the organisation undertakes to the individual that it will not disclose the information without the individual's consent.

19.6 NPPs 10.2, 10.3 and 10.4 regulates the collection of health information by organisations. Health information is a category of sensitive information. Issues concerning the collection of health information are discussed in Part H.

Expansion of sensitive information principle to agencies?

Background

19.7 The fact that the IPPs do not contain a principle dealing specifically with sensitive information is consistent with the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), which also do not contain such a principle. Indeed, the Explanatory Memorandum to the OECD Guidelines states that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[7] On the other hand, as noted above, the EU Directive deals with 'special categories of data', which are defined as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'.[8] Article 8 prohibits the processing of this kind of information without consent, except in specified circumstances. It also allows member states to prohibit the processing such data, even with the consent of the data subject.

19.8 In light of the above, it is necessary to consider whether agencies should also be subject to superadded restrictions in relation to the collection of sensitive information. This issue was identified in the ALRC's Issues Paper, *Review of Privacy* (IP 31).[9]

19.9 For the purpose of comparison, it should be noted that some other Australian jurisdictions regulate how government agencies should deal with sensitive information. For example, under Victorian, Tasmanian and Northern Territory privacy legislation,

---

6 Non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims. See *Privacy Act 1988* (Cth) sch 3, NPP 10.5.

7 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19(a)].

8 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

9 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–32 and [4.181].

agencies are subject to restrictions in relation to the collection of sensitive information.[10]

Submissions and consultations

19.10 A number of stakeholders submitted that agencies, like organisations, should also be subject to a 'sensitive information' privacy principle.[11]

19.11 The Australian Government Department of Health and Ageing noted that the NPPs currently contain an exception to the prohibition on collecting sensitive information where it 'is required by law'. There is no exception, therefore, where the collection is merely authorised, but not required, by law. It submitted that the absence of an exception where the collection is authorised by law would 'impose significant limitations on agencies' by, for instance, preventing agencies from collecting sensitive information from third parties unless specifically required to do so. Therefore, the Department's preferred position is that there be an exception to the prohibition on collecting sensitive where the collection is required *or authorised* by law. It was noted that such an amendment would render the provision currently in NPP 10.2 redundant.[12]

ALRC's view

19.12 The ALRC shares the view of many stakeholders that the privacy principle dealing with sensitive information should be extended to cover agencies as well as organisations.

19.13 The term 'sensitive information' is defined in s 6(1) of the *Privacy Act* as a finite list of categories of personal information. These categories of information have been treated differently from other forms of personal information because, if misused, the information can be especially damaging to the individual concerned or those associated with the individual. As explained in Chapter 3, misuse of sensitive information—such as information about an individual's ethnic origin or religious beliefs—is especially dangerous because it can give rise to grave consequences, including discrimination and other forms of mistreatment.

19.14 Generally speaking, there is a correlation between the categories of sensitive information provided for in the *Privacy Act* and the grounds of discrimination provided for under federal and state legislation.[13] Similarly, Australia's international law obligations are triggered by an asylum seeker who has a well-founded fear of persecution by reason of his or her 'race, religion, nationality, membership of a

---

10 *Information Privacy Act 2000* (Vic) sch 1, IPP 10.1; *Personal Information Protection Act 2004* (Tas) sch 1, IPP 10(1); *Information Act 2002* (NT) sch, IPP 10.1.

11 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

12 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

13 Compare *Privacy Act 1988* (Cth) s 6(1) with, eg, *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Disability Discrimination Act 1992* (Cth).

particular social group or political opinion'.[14] The fact that three of these grounds—race, religion and political opinion—are also categories of 'sensitive information' in s 6(1) of the *Privacy Act* reflects the inherent dangers that may arise where personal information of this nature is misused.

19.15 There are, therefore, strong policy reasons to require agencies, and not just organisations, to abide by a privacy principle dealing with sensitive information. The ALRC is of the view that the risks associated with this information being subsequently misused are sufficiently serious that agencies should also be required to abide by the superadded requirements that apply to the collection of sensitive information.

19.16 Nevertheless, any such principle, especially if it is made applicable to agencies, must be structured in such a way as to allow for collection by agencies of sensitive information for legitimate reasons. The ALRC acknowledges the force of the submission made by the Australian Government Department of Health and Ageing that the provision that allows a data collector to collect sensitive information if the collection is required by law is too narrow.

19.17 Consistently with the discussion in Chapter 13, the ALRC is of the view that it would be appropriate to broaden this provision so that it applies where the collection of sensitive information is required or specifically authorised by or under law. In particular, this would encourage the Australian Parliament or relevant Minister to balance the competing interests for and against the collection of sensitive information in a particular context and, where appropriate, to pass primary or subordinate legislation permitting such collection, subject to whatever conditions are deemed appropriate.

19.18 A further miscellaneous question relates to the drafting of the proposed UPPs—that is, where should the provisions dealing with the collection of sensitive information be placed? In other words, should these provisions appear in a separate privacy principle, as is currently the case in NPP 10, or should they be located in the proposed 'Collection' principle, given that the provisions only relate to the *collection* of sensitive information, and not other aspects of the information cycle. This issue was not the subject of a question in IP 31, nor was it the subject of any significant feedback from stakeholders.

19.19 The ALRC's view is that it would be clearer to locate the provisions dealing with the collection of both forms of personal information—that is, sensitive and non-sensitive information—in a single privacy principle called 'Collection' in the proposed UPPs. There seems no reason in policy to deal with the collection of sensitive

14 See *Migration Act 1958* (Cth) s 36, incorporating the *Convention relating to the Status of Refugees*, 28 July 1951, [1954] ATS 5, (entered into force generally on 22 April 1954).

information in a separate privacy principle. Moreover, retaining a separate sensitive information principle can imply that there is a completely separate regime for all aspects of handling sensitive information. As explained below, however, the ALRC explicitly opposes such an approach.

Proposal 19–1 The proposed Unified Privacy Principles should set out the requirements on agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*. These requirements should be located in the proposed 'Collection' principle.

Proposal 19–2 The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or specifically authorised by or under law.

Regulation of other aspects of sensitive information handling

Background

19.20 As noted above, the IPPs do not impose special restrictions on the collection of sensitive information; nor do they distinguish between the treatment of sensitive information and non-sensitive information in other stages of the information cycle such as use, disclosure, access, retention and disposal. Guidelines issued by the Office of the Privacy Commissioner (OPC) expressly acknowledge that where sensitive information is concerned, 'more care to protect individuals' privacy may be appropriate than is required by the letter of the IPPs'.[15]

19.21 NPP 10 imposes restrictions on the collection of sensitive information, and, as discussed in Chapter 22, NPP 2 distinguishes between sensitive and non-sensitive personal information in the context of use and disclosure. The NPPs, however, do not impose separate requirements for the handling of sensitive information in all aspects of the information cycle.

19.22 In this regard, it is relevant to note that some jurisdictions, like New Zealand, do not distinguish between the treatment of sensitive and non-sensitive personal information.[16] Equally, however, others like the United Kingdom and Germany, do set up separate regimes for sensitive and non-sensitive information.[17] New South Wales

15 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 1.

16 See *Privacy Act 1993* (NZ).

17 See *Data Protection Act 1998* (UK) sch 1, Principle 1; sch 3; *Federal Data Protection Act 1990* (Germany).

privacy law also distinguishes between the disclosure of sensitive and non-sensitive information.[18]

19.23 In this context, the ALRC asked in IP 31:

> Should federal privacy principles establish a separate regime for the public and private sectors regulating sensitive information in all aspects of the information cycle, including collection, use, disclosure, storage, access, retention and disposal? If so, what should that regime include?[19]

19.24 There appear to be three main options for reform, in addition to maintaining the status quo. These are to create a:

- privacy principle that obliges more care to be taken with respect to sensitive information, and also to amend other privacy principles by setting out how sensitive information should be dealt with as relevant to the principle in question;

- privacy principle that comprehensively covers the obligations that apply when handling sensitive information at any stage of the information cycle; or

- completely separate statutory regime for the handling of sensitive information that is outside of the privacy principles.[20]

Submissions and consultations

19.25 The starting point for a number of stakeholders was the community expectation that 'sensitive information will be afforded special privacy protections above and beyond ordinary, non-sensitive personal information'.[21] There is less consensus, however, on how this can best be achieved.

19.26 Some stakeholders submitted that the rules relating to sensitive information should be articulated with reference to all aspects of the information cycle, but did not specify a preferred model for achieving this.[22]

19.27 In terms of the model for reform, the OPC favoured a privacy principle that comprehensively covers the obligations that apply when handling personal information

---

18 *Privacy and Personal Information Protection Act 1998* (NSW) ss 18, 19.

19 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–32.

20 An example of such a regime is Part VIA of the *Privacy Act*, which deals with declared emergencies.

21 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; AAMI, *Submission PR 147,* 29 January 2007.

22 AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

at any stage of the information cycle. It submitted that amendments should be made to the other privacy principles to complement the sensitive information principle and to draw attention to the 'special nature of sensitive information' and the obligations that apply with respect to it.[23] Specifically, it submitted that the following consequential amendments should be made:

- The collection principle could consider requiring express/explicit consent, when dealing with sensitive information.
- With regard to use and disclosure, the circumstances of 'authorised' by law, could be strengthened. Specifically, to avoid a broad reading of this where sensitive information is at stake, the inclusion of 'clearly' or 'expressly' authorised could be considered.
- The security and data quality principles … could recognise the special character of sensitive information, through the inclusion of 'having regard to the sensitive nature of the information'.
- The security and data quality principles may also serve to clarify what obligations organisations/agencies are under when handling sensitive information.[24]

19.28 The Government of South Australia submitted that the relevant privacy principle could be supplemented by other law and guidance. It was suggested, for example, that public and private sector bodies should be required to comply with the *Australian (and International Standard) for Records Management*.[25]

19.29 On the other hand, a large number of stakeholders submitted that it would be preferable simply to maintain the status quo.[26] It was argued, for instance, that instituting a separate regime for handling sensitive information 'would unnecessarily complicate' this area.[27]

ALRC's view

19.30 The ALRC is of the view that, if the other proposals in this Discussion Paper are adopted, it would unnecessary to include any further provisions in the proposed UPPs to deal with sensitive information. The ALRC takes this view for the following reasons.

19.31 First, a number of the amendments proposed by the OPC would be, arguably, unnecessary if the UPPs are adopted in the manner proposed by the ALRC. That is:

---

23 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

24 Ibid.

25 Government of South Australia, *Submission PR 187,* 12 February 2007.

26 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

27 Australian Federal Police, *Submission PR 186,* 9 February 2007. See also Law Council of Australia, *Submission PR 177,* 8 February 2007.

- The OPC suggested a strengthening of the consent requirement in respect of the collection of sensitive information. However, ensuring that consent is 'genuine' or 'real' could be dealt with by Proposal 16–1. As explained in Chapter 16, the problems regarding consent may be solved more effectively by adopting a contextual approach to consent, and providing further guidance from the OPC about what is required to obtain consent in various situations.

- The OPC suggested that the exception to the secondary purpose use and disclosure prohibition where the use or disclosure is 'authorised by or under law' (NPP 2.1(g)) should be amended in respect of sensitive information to apply where the use or disclosure is *clearly or expressly* authorised by or under law. As noted in Chapter 22, the ALRC is interested in views about whether the equivalent provision in the proposed UPPs should apply where the use or disclosure is 'required or *specifically* authorised by or under law'.[28]

- It was suggested that the principles dealing with data quality and data security should be strengthened and clarified with respect to sensitive information. As explained in Chapter 25, the ALRC proposes some strengthening of the proposed 'Data Security' principle and also further guidance from the OPC on how to comply with these requirements. The ALRC believes that this, in combination with a relevance requirement in the proposed 'Data Quality' principle,[29] would be sufficient to deal with concerns relating to sensitive information.

19.32 Secondly, as discussed in Chapter 23, the ALRC proposes that the provision in NPP 2.1(c) that precludes sensitive information from being used in secondary purpose direct marketing should be retained in the proposed 'Direct Marketing' principle. This provides a measure of protection that is particularly important to stakeholders. It also shows that, to some extent, the UPPs will deal with sensitive information separately, outside the collection context.

19.33 Thirdly, the ALRC proposes in Part H that the provisions in the current NPPs that relate only to health information—which is a particularly important type of sensitive information—should be moved into the proposed *Privacy (Health Information) Regulations*, rather than being dealt with under the UPPs. These Regulations will set out rules that are tailored to this particular type of sensitive information.

19.34 Finally, the ALRC notes that a large number of stakeholders have indicated that they are against the establishment of a separate regime for the handling of sensitive

---

28 See Question 22–1.
29 See Proposal 24–2.

information. Such a regime could involve significant compliance costs, in circumstances where the most dangerous risks with respect to sensitive information are dealt with at the initial stage of collection.

Emergency situations

19.35 In IP 31, the ALRC solicited views as to whether the current exceptions to the prohibition on collection of sensitive information are adequate and appropriate.[30] For example, in the context of the disclosure principle in IPP 11 and the use and disclosure principle in NPP 2, the requirement that there be a 'serious *and* imminent' threat to the life or health of an individual poses difficulties in practice because often it may only be possible to establish a serious *or* imminent threat. Particularly in the case of disaster recovery, the threat may be serious but no longer 'imminent'. AAMI, for example, submitted that agencies should be able to collect sensitive information in emergency situations.[31]

19.36 Given that similar wording is used in one of the exceptions in NPP 10, there is a question whether the principle dealing with sensitive information should specifically allow for the collection of sensitive information in emergency situations, including disaster recovery, where the individual is not in a position to give consent. It should be noted, however, that after the release of IP 31, the *Privacy Act* was amended to insert a new Part VIA, which commenced operation on 7 December 2006.[32] Part VIA displaces some of the requirements in the IPPs and NPPs by providing a separate regime for the collection, use and disclosure of personal information where there is a connection to an emergency that has been the subject of a declaration by the Prime Minister or a Minister. It may be that the new Part VIA responds adequately to the concerns in relation to this aspect of the sensitive information principle. The Part VIA regime is considered in detail in Part E.

19.37 In comparison, German privacy law specifically allows for the collection by public bodies of 'special categories of personal data' where: it is 'urgently needed to protect an important public interest'; 'it is urgently necessary in order to avert serious prejudice to the public interest or to safeguard important public interest concerns'; or 'it is necessary on compelling grounds relating to … obligations of the Federal Government in the area of crisis management or … for humanitarian measures'.[33]

ALRC's view

19.38 The ALRC's view is that the exception in NPP 10.1(c) should be relaxed to some extent. For the reasons set out in Chapter 22, the requirement that the threat must

30 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.184].
31 AAMI, *Submission PR 147,* 29 January 2007.
32 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).
33 *Federal Data Protection Act 1990* (Germany) s 13.

be both serious *and* imminent is too difficult to satisfy and it can lead to personal information not being used or disclosed in circumstances where it should be.[34]

19.39 The ALRC believes that the exception should be triggered where a threat is merely serious, but not necessarily imminent. This would allow an agency or organisation to take preventative action to stop a threat from developing to a crisis. As a number of stakeholders have observed, at that point, it is often too late to take meaningful action. The ALRC also believes that this formulation strikes an appropriate balance between respecting the privacy rights of an individual and the public interest in averting threats to life, health and safety.

19.40 Moreover, it should be noted that NPP 10.1(c) imposes additional requirements before an organisation can avail itself of this exception to the prohibition against collecting sensitive information. That is, the individual concerned:

> (i) is physically or legally incapable of giving consent to the collection; or
>
> (ii) physically cannot communicate consent to the collection.[35]

19.41 In other words, this exception only applies where the individual is incapable of giving consent. As discussed in Part I, the term 'incapable' in this context includes the situations referred to in NPP 10.1(c)(i) and (ii). The ALRC believes that this condition should be retained in the relevant provision in the proposed UPPs.

Proposal 19–3 The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent.

Emergency situations not involving a serious threat to life or health

19.42 The Community Services Ministers' Advisory Council (CSMAC) raised concern about the provision of services to vulnerable people who are unable to provide informed consent.

> A person may have impaired competence (either short or long term) to provide informed consent and there is no alternative consent provider, such as a legal guardian or family member. This is a frequent dilemma for homeless services, where the capacity to provide informed consent may be limited by factors such as the use of substances or mental health problems. In such circumstances, there is a dilemma

34 See, in particular, Proposal 22–3 and accompanying text.
35 *Privacy Act 1988* (Cth) sch 3, NPP 10.1(c).

> about how to treat consent: a person might provide consent which is of dubious validity, or alternatively, may refuse consent but with a limited understanding of either the consent or the implications of their refusal, which may affect their treatment or access to services that they have requested.[36]

19.43 This is a particular problem where a service cannot be provided without the collection of relevant sensitive information. In accordance with Proposal 19–3 above, where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, collection should be allowed to occur without the consent of the individual concerned.

19.44 The CSMAC raised further questions about whether certain services fall within the definition of 'necessary to lessen or prevent a serious threat to life or health'. For example, those running accommodation services for homeless individuals will sometimes need access to information about the health of the individual before providing accommodation to an individual. The CSMAC queries whether a mere decline in health, or the dangers associated with sleeping rough, would be considered a 'serious threat to life or health', or whether a crisis event is required to trigger the exception. It notes that many err on the side of caution in making these interpretations, thus affecting the accessibility of services for vulnerable individuals.[37]

19.45 The ALRC agrees that there are valid arguments for extending the exception to the consent requirement for collection of sensitive information to circumstances beyond the need to 'lessen or prevent a serious threat to life or health of an individual'. One suggestion is to allow collection where it is necessary to provide an essential service for the benefit of the individual, and further limit the exception by requiring the collection to be reasonable in all the circumstances. Any extension of the existing exception may, however, have unintended consequences. The ALRC is, therefore, seeking stakeholder input before reaching a conclusion on this issue. The ALRC welcomes comments on the general concept of the extension of the exception, as well as suggestions for an appropriately framed exception.

Question 19–1 Should the proposed sensitive information provisions provide that sensitive information can be collected where all of the following conditions apply:

36 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.
37 Ibid.

(a) the individual is incapable of giving consent;

(b) the collection is necessary to provide an essential service for the benefit of the individual; and

(c) the collection would be reasonable in all the circumstances?

Research

19.46 In some state and territory privacy legislation, there is a research-related exception to the prohibition on collection of sensitive information by agencies, and this is broader than that provided for in NPP 10. For example, in Victoria and the Northern Territory, public sector bodies can collect sensitive information—not just health information—if:

- the collection is necessary for research, the compilation or analysis of statistics relevant to government funded targeted welfare or educational services, or relates to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services;[38]

- there is no other reasonably practicable alternative to collecting the information for that purpose; and

- it is impracticable for the organisation to seek the individual's consent to the collection.[39]

19.47 This raises the question whether the sensitive information privacy principle should permit the collection of non-health related sensitive information for certain purposes, including research and statistical purposes, and in what circumstances this should be permitted. This question is dealt with separately in Part H.

38 See also *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).
39 *Information Privacy Act 2000* (Vic) sch 1, IPP 10.2; *Information Act 2002* (NT) sch, IPP 10.2.

20. Specific Notification

Contents

Introduction 627
Location of notification requirements: separate principle? 628
Submissions and consultations 628
ALRC's view 629
Notification of collector's identity and individual's rights 630
Submissions and consultations 631
ALRC's view 631
Notification of the fact and circumstances of collection 633
ALRC's view 634
Standardising requirements of agencies and organisations 635
Submissions and consultations 636
ALRC's view 638
Notification where information collected from a third party 640
Background 640
Submissions and consultations 641
ALRC's view 642
Meaning of 'reasonable steps' 645
Submissions and consultations 646
ALRC's view 647
Summary of proposed 'Specific Notification' principle 648

Introduction

20.1 The privacy principles in the *Privacy Act 1988* (Cth) provide that, in certain circumstances, agencies and organisations are required to notify an individual whose personal information has been, or is to be, collected, of a number of specific matters. This form of notification is referred to in this Discussion Paper as 'specific notification' because it is specific to the individual and the personal information in question. It may be contrasted with the 'openness' requirements on agencies and organisations.[1] Those are fulfilled by agencies and organisations making available their privacy policy, setting out their approach to handling personal information generally. In other words, it is not linked to any one individual's personal information.

1 The 'openness' requirements are discussed in Ch 21.

20.2 Currently, most of the requirements relating to notification are dealt with in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) relating to the collection of personal information. That is, IPP 2 provides that where an agency solicits personal information directly from the individual concerned for inclusion in a record or in a generally available publication, it must take reasonable steps to ensure that, before or soon after the information is collected, the individual is generally aware of:

- the purpose for which the information is being collected;
- if the collection is authorised or required by law—that fact; and
- to whom it is the agency's usual practice to disclose or pass on personal information of the kind collected.

20.3 Similarly, NPP 1.3 provides that an organisation may only collect personal information from an individual after taking reasonable steps to ensure the individual is aware of: the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; the organisations to whom the organisation usually discloses information of that kind; any law requiring the particular information to be collected; and the main consequences for the individual if the information is not provided.

20.4 This chapter is concerned with four main questions. First, should the requirements relating to specific notification be set out in a separate privacy principle? Secondly, what should be agencies' and organisations' specific notification requirements? Thirdly, what specific notification requirements should apply where personal information is received by an agency or organisation from a third party (a person other than the individual concerned)? Finally, how are agencies and organisations expected to fulfil these requirements?

Location of notification requirements: separate principle?

20.5 As noted above, the specific notification requirements are currently set out in the privacy principles that deal with the collection of personal information. A question arises as to whether the proposed Unified Privacy Principles (UPPs) should continue to set out the notification requirements that apply at or around the time the information is collected in the 'collection' privacy principle, or whether these requirements should be dealt with in a separate specific notification principle.

Submissions and consultations

20.6 A number of stakeholders submitted that notification requirements should be located in a separate privacy principle that deals with notification (or 'notice') and

openness.[2] One submission argued that this would facilitate 'a more pragmatic discussion of the desirable levels of awareness, and how and when these can be created'.[3]

20.7 The Office of the Privacy Commissioner (OPC) pointed to the fact that notification is treated as a separate privacy principle in, among other instruments, the Asia-Pacific Economic Cooperation *Privacy Framework* (2005),[4] and the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995).[5]

20.8 The OPC suggested a joint 'notice and openness' privacy principle and that this should be listed before the 'collection' principle in the UPPs to encourage data collectors to consider their 'stated reasons' for collection, use and disclosure *before* collecting the personal information in question.[6]

ALRC's view

20.9 In the ALRC's view, the requirements on agencies and organisations to provide specific notification to an individual of particular matters relating to the collection or handling of personal information about the individual should be consolidated in a single, discrete privacy principle. This would clarify the present position under the IPPs and NPPs, where the requirements relating to specific notification are dealt with as issues subservient to the collection of personal information. As a consequential amendment, the 'Collection' principle in the proposed UPPs has been drafted to include a reference to the fact that agencies and organisations are required to comply with the relevant specific notification requirements when they collect personal information.[7]

20.10 The second issue that is raised here is whether the requirements relating to specific notification (that is, the matters currently dealt with in IPP 2 and NPP 1.3, and which are the subject of this chapter) should be dealt with in the same privacy principle as the requirements relating to openness (that is, the matters currently dealt with in

---

2 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

3 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

4 See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle II.

5 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995) arts 10–11.

6 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A similar submission was made by G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

7 See UPP 2.4—the UPPs are set out at the beginning of this Discussion Paper.

IPP 5 and NPP 5, and which are the subject of Chapter 21). As noted below, some stakeholders have proposed such an arrangement.[8]

20.11 The ALRC believes that there is an important conceptual difference between the current openness principles (IPP 5 and NPP 5) and what are referred to in this Discussion Paper as the specific notification principles (IPP 2 and NPP 1.3). On one hand, the openness principles require individuals to be informed about the *general* practices of an agency or organisation in relation to the handling of personal information. As such, these requirements apply irrespective of whether the agency or organisation has actually collected personal information from a particular individual, or whether the agency or organisation simply might do so in the future. On the other hand, the specific notification principles apply when personal information has been, or will soon be, collected from a particular individual. Consequently, these principles require the agency or organisation to notify an individual about how it will handle certain, specified personal information relating to the individual.

20.12 In other words, the conceptual difference between the 'openness' principle and the provisions of IPP 2 and NPP 1.3 may be summarised as follows: the openness principle requires notification as to the general practices of an agency or organisation relating to the handling of *any* personal information, whereas IPP 2 and NPP 1.3 require notification as to how an agency or organisation will handle an individual's *particular* personal information. As set out in Chapter 21, the ALRC therefore believes that it is preferable to deal with specific notification in a privacy principle separate from the principle dealing with 'openness'.

Proposal 20–1 The proposed Unified Privacy Principles should contain a principle called 'Specific Notification' that sets out the requirements on agencies and organisations to provide specific notification to an individual of particular matters relating to the collection and handling of personal information about the individual.

Notification of collector's identity and individual's rights

20.13 IPPs 1–3, taken together, contain a significant gap relating to notification when compared with NPP 1. Where an organisation collects personal information about an individual, NPP 1 expressly requires the organisation to 'take reasonable steps' to ensure the individual is aware of: the collector's identity and contact details; the fact that the individual is able to gain access to the information; and the main consequences of not providing the information. The IPPs contain no equivalent requirement applicable to agencies.

8 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

20.14 In other jurisdictions, such as New Zealand, government bodies are required to make an individual aware of the collector's identity and contact details, as well as the fact that the individual can access the information. There are also significant consequences if a government body fails to provide the information.[9] In light of this gap, the ALRC asked whether these notification obligations, currently located in NPP 1, should be extended to agencies.[10]

Submissions and consultations

20.15 The majority of stakeholders who responded to this question supported such an amendment to bring the notification requirements of agencies in line with those that currently apply to organisations.[11]

20.16 One submission suggested that such a provision has become necessary because it is now more difficult for individuals to know which government agency they are dealing with, given the 'increasing use of campaign names and brands by the public sector and with ever-changing administrative arrangements and "portfolios"'.[12] The OPC also supported this reform. It argued, however, that any such requirements should be consolidated with the other notification requirements and placed in a separate privacy principle.[13]

20.17 There were, however, a small number of stakeholders that opposed this reform.[14] One stakeholder argued that it would place an unreasonable impediment on law enforcement agencies.[15]

ALRC's view

20.18 Provided the notification requirements are subject to appropriate qualifications, the ALRC can see no policy reason why agencies that collect personal information should not generally be subject to the same specific notification requirements that

---

9 See *Privacy Act 1993* (NZ) s 6, Principles 3(1)(d), (f), (g).

10 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–3.

11 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

12 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007

13 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

14 Australian Federal Police, *Submission PR 186,* 9 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

15 Confidential, *Submission PR 165,* 1 February 2007.

apply to organisations. On the contrary, such notification requirements promote fairness and transparency. Moreover, insofar as specific notification brings the fact that a particular agency has collected information to the attention of the individual concerned, it can also promote accurate record-keeping because the individual would be more likely to access the information to check its accuracy.

20.19 The addition of such requirements would benefit individuals. As explained above, the provisions relating to openness serve a different purpose. Further, many individuals find general privacy notices confusing, too long and difficult to relate to their particular situation.[16] Professor Fred Cate criticised modern privacy notices, by stating:

> Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice.[17]

20.20 In contrast, where notification requirements are tailored to the specific personal information in question, they can be shorter, clearer and more easily related to the individual's own circumstances. Moreover, providing an individual with specific notification about matters relating to the collection of his or her personal information can be particularly useful and timely because this may be the most appropriate time for the individual to take any action to protect his or her privacy.

20.21 The main disadvantage of expanding the specific notification requirements applicable to agencies seems to be that notifying an individual of the relevant matters at the time of collecting his or her personal information could, in certain circumstances, undermine an agency's legitimate purpose in collecting the information in the first place. The example noted above from submissions and consultations is that, in a law enforcement context, notification of personal information collection may, for instance, 'tip off' a suspect that he or she is under surveillance, thereby frustrating the legitimate functions of the agency in question.

20.22 To some extent, the solution to this problem may already be provided for in NPP 1. That is, both NPP 1.3 (which applies to information collected from the individual in question) and NPP 1.5 (which applies to information collected from a third party) qualify the notification requirements by stating that an organisation must 'take reasonable steps' to notify the individual of the relevant matters. In such situations, it may be argued that 'reasonable steps' would equate to the agency doing nothing at all. As explained later in this chapter, however, there is some confusion regarding the meaning of the term 'reasonable steps'. Moreover, it is arguably disingenuous to say that an agency has fulfilled the 'reasonable steps' requirement to

---

16 See, eg, Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 39.

17 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 1.

make an individual aware of certain matters where the agency is avowedly seeking to *avoid* making the individual aware of those matters.

20.23 To avoid any potential ambiguity, therefore, the ALRC proposes two further measures to cover more directly the situation where an agency legitimately wishes not to make an individual aware of the specified matters at or around the time personal information is collected. First, the ALRC believes that the principle should contain a qualification stating that an agency is not required to comply with the relevant notification requirements if the collection is 'required or specifically authorised by or under law'. This solution strikes an appropriate balance between making agencies generally accountable for the personal information they collect and recognising that, in certain situations, the requirements of accountability and transparency should be relaxed in favour of another consideration that must take precedence.

20.24 Secondly, the ALRC proposes a further qualification that would be applicable both to agencies and organisations. That is, the ALRC believes that the specific notification requirements should apply only in circumstances where a reasonable person would expect to be notified. The addition of this objective test would permit a more common sense approach to be taken in deciding whether an agency or organisation is obliged to fulfil the specific notification obligations in a particular case. This is discussed in greater detail below.

20.25 If these proposals are adopted, a further consequential amendment would be needed to import into the UPPs a provision, which is also applicable to agencies, that is equivalent to the current NPP 1.5. NPP 1.5 provides that where an organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in NPP 1.3, except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual. Consistently with the approach taken in this chapter, including Proposal 20–5 below, this provision should apply to agencies as well as organisations, but agencies should retain an exception stating that the specific notification requirements would not apply to an agency if an agency is required or specifically authorised by or under law not to make the individual aware of such matters.

Notification of the fact and circumstances of collection

20.26 Neither the IPPs nor the NPPs require an agency or organisation to notify an individual that it has collected, or is about to collect, personal information about that individual. It is arguably implicit in the existing specific notification provisions that the agency or organisation needs to provide the individual with notice that his or her personal information has been collected.

20.27 On the other hand, given the growing ability for technology to facilitate the collection of personal information about an individual without the individual knowing that this has occurred, it may be desirable for agencies and organisations to be required to notify individuals of the fact and circumstance of the collection of their personal information.[18] It should be noted that although the ALRC's Issues Paper, *Review of Privacy* (IP 31) did not contain any question specifically directed to this issue, some stakeholders commented on the issue in consultations and submissions.

20.28 AAMI, for example, opposed the 'covert' collection of personal information, submitting that 'methods of collection need to be foreseeable'.[19] The Victorian Society for Computers and the Law (VSCL) noted that certain types of biometric information, such as iris scanning collected for the purposes of inclusion in a biometrics template, are likely to require the active cooperation of the individual in the process of collection. In comparison, biometrics such as facial and voice recognition may be collected without the knowledge or consent of the individual. In some circumstances, therefore, the consent (or, at least, the knowledge) of the relevant individual may be implied in the privacy principles governing collection.[20]

20.29 The VSCL also noted that rapid developments in technology—including in the field of biometrics systems—may result in the widespread availability of technologies that are capable of collecting personal information without the knowledge of the individual.[21] Other technologies, such as invisible data collecting devices on web pages or hidden radio frequency identification (RFID) tags, already may be collecting personal information without the knowledge or consent of the individual.

ALRC's view

20.30 The ALRC agrees with the VSCL's observation that emerging technologies make it possible to acquire various types of personal information without an individual's knowledge. The ALRC's view is that, subject to certain qualifications discussed below, agencies and organisations should be required to notify an individual that they have collected the individual's personal information and the circumstances in which this collection took place.

20.31 The ALRC believes that this would have a number of benefits. For example, it would better equip individuals to protect their personal information. By knowing that their personal information has been collected, they would be able to take action to safeguard that information—for example, by checking its accuracy. Another benefit is that it would help agencies and organisations to be more transparent in their data collection processes.

---

18 The impact of developing technologies on privacy is discussed in Part B.
19 AAMI, *Submission PR 147,* 29 January 2007.
20 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.
21 Ibid.

20.32 The main potential problem with adding a requirement to notify individuals of the fact and circumstances of collection seems to be that often individuals are already aware that their personal information is collected—indeed, they may have provided the information themselves. In these circumstances, arguably it would be both pointless for the individual and onerous on agencies and organisations to notify individuals that their personal information has been collected.

20.33 The ALRC believes, however, that the qualifications and exceptions to this requirement, which are built into the proposed 'Specific Notification' principle, adequately address these concerns. In particular, the ALRC proposes that agencies and organisations should be required to comply with the relevant specific notification obligations only in circumstances where a reasonable person would expect to be notified.[22] If an individual is already aware that his or her personal information has been collected, clearly it would not be necessary for the agency or organisation to notify him or her. A similar point has been made by Professor Fred Cate:

> If the collection from data subjects is not reasonably obvious, then there should be prominent notice of the fact. If data collection is reasonably obvious, additional notice requirements are superfluous.[23]

20.34 Consequently, subject to relevant qualifications and exceptions, the ALRC's view is that, where an agency or organisation collects personal information about an individual, it should be required to notify the individual of the fact and circumstances of that collection. This is set out in Proposal 20–2 below.

Standardising requirements of agencies and organisations

20.35 In IP 31, it was noted that the IPPs and NPPs do not uniformly require agencies and organisations that collect personal information about an individual to notify the individual in question about certain matters. In particular, the IPPs do not require an agency to notify an individual of the types of people, bodies or agencies to whom the agency usually discloses personal information. Further, neither the IPPs nor NPPs require an agency or organisation to notify an individual of the avenues of complaint available when personal information is collected.

20.36 The ALRC asked whether some or all of these obligations should be imposed on agencies and/or organisations.[24]

---

22 See Proposals 20–2 and 20–5.

23 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 30.

24 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–1, 4–3.

Submissions and consultations

20.37 A number of stakeholders who responded to this general question argued that agencies and organisations should be required to provide both categories of information listed above.[25]

20.38 There were, however, some who either opposed such notification requirements or expressed reservations. Some suggested that the existing notification requirements are adequate and there are few complaints relating to insufficient notification.[26] It was also submitted that such requirements would 'significantly add to the length of privacy notices', which does not benefit consumers.[27] Telstra argued that the cost of compliance would be undesirably onerous.[28]

20.39 While not expressing outright opposition to these extended notification requirements, some reservations were expressed, including that:

- where personal information is collected via a call centre, for practical reasons, notification should not have to be oral because this would be too time consuming;[29]

- such notification requirements should not apply where it is 'impracticable or inappropriate' to notify the individual;[30] and

- where notification would be to a large number of people, such as the individuals listed on a large public database, Veda Advantage submitted that data aggregation specialists should be allowed to use 'appropriate' notification methods that are widely publicised and available. These may include providing details on a searchable industry website or by other notice.[31]

Notification of entities to whom information usually disclosed

20.40 It should first be noted that, under NPP 1.3(d), an organisation is already obliged to notify an individual of the types of people, bodies or agencies to whom the

---

25 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

26 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; ANZ, *Submission PR 173,* 6 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

27 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007. A similar point was made by: Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; ANZ, *Submission PR 173,* 6 February 2007.

28 Telstra, *Submission PR 185,* 9 February 2007.

29 AAMI, *Submission PR 147,* 29 January 2007.

30 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

31 Veda Advantage, *Submission PR 163,* 31 January 2007.

organisation usually discloses such information. There are, therefore, three questions that arise. The first is whether agencies should also be subject to such a requirement. A number of stakeholders supported such an amendment.[32] None specifically opposed it.

20.41 The second question is whether any amendment should be made to the scope of this requirement. Specifically, NPP 1.3 only requires an organisation to ensure that an individual is aware of the 'organisations' to which it usually discloses information of that kind. However, 'organisation' currently has a restricted meaning for the purposes of the *Privacy Act*, excluding, for example, political parties and state or territory agencies. The OPC recommended in 2005 that the Australian Government consider amending NPP 1.3(d) to extend its coverage to disclosures generally, including to public sector agencies of the Australian Government, state or local governments, other bodies and private individuals.[33] The only stakeholder that commented specifically on this issue supported such an expansion.[34]

20.42 The third question assumes that such a requirement is adopted and asks: what level of specificity is required when providing this notification? Problems have arisen where this notification is too general, such as where an insurer notified an individual that it may disclose personal information to 'a Mediator, Solicitor, Complaints Resolution Tribunal or Court or to any other person necessary for claims determination purposes'.[35] It was submitted that such a description was too broad to be useful to an individual in determining whether to proceed with the transaction in question.[36] This led to the suggestion that data collectors should be permitted to give such descriptions, but they should also be required to answer any specific inquiry as to whether an entity actually received personal information.[37]

Notification of avenues of complaint

20.43 There is strong support for requiring agencies and organisations to make individuals aware of the avenues of complaint available when personal information is collected. The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) recommended that the Australian Government consider amending NPP 1.3

---

32 See, eg, Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

33 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 74. Note, however, that the definition of 'organisation' extends to individuals.

34 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

35 *N v Private Insurer* [2004] PrivCmrA 1.

36 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

37 G Greenleaf and N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

along these lines.[38] A number of stakeholders supported such a requirement.[39] In supporting such reform, the Australian Privacy Foundation stated that the principle should require notification of 'both internal and external dispute resolution options'.[40]

20.44 There was, however, some opposition. The Australian Bankers' Association submitted that the *Privacy Act* should not impose such an obligation on organisations, because banks and holders of Australian Financial Services Licences are already subject to similar requirements under the *Corporations Act 2001* (Cth) and/or the Code of Banking Practice.[41]

ALRC's view

Notification of entities to whom information usually disclosed

20.45 The ALRC's view is that, where an agency or organisation collects personal information about an individual, it should be required to notify the individual of the types of people, organisations, agencies or other entities to whom it usually discloses personal information. As already noted, NPP 1.3(d) already imposes a similar requirement on organisations. The ALRC notes that there was general support for the expansion of this general requirement to apply also to agencies.

20.46 Regarding the content of the requirement, NPP 1.3(d) only requires notification of the *organisations* to which the information is usually disclosed. The OPC Review recommended, however, that notification should extend to other bodies that do not fall within the definition of 'organisation'—most notably, agencies and state and territory bodies.[42] The OPC stated that a narrow interpretation of this requirement seems inconsistent with the policy intent of the legislation, given that the Explanatory Memorandum envisaged disclosure to state government licensing authorities, which do not fall within the definition of 'organisation'.[43]

20.47 There was no specific opposition to such an expansion. The ALRC supports such an amendment, particularly in light of the fact that it would appear to correlate better with the original intention of the provision. Moreover, it would be unlikely to cause a significant compliance burden, given that this obligation already seems to be operating adequately for organisations.

---

38 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 41.

39 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

40 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

41 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

42 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 74.

43 See Ibid, 259; Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [3.34].

20.48 The final question is: what level of specificity is required when providing this notification? The ALRC acknowledges the problems noted above, where notification has been too general to be of real assistance to individuals. Consistently with the desire to frame the UPPs using principles (as distinct from detailed, prescriptive provisions),[44] however, the ALRC does not believe that the relevant privacy principle should prescribe what level of detail is required in notification. Rather, the OPC should provide guidance to assist agencies and organisations to comply with the principle.

Notification of avenues of complaint

20.49 As noted above, there is strong support among stakeholders for requiring an agency or organisation to make an individual aware of the avenues of complaint available when it collects personal information about the individual. Such a requirement is desirable because it would assist individuals in enforcing their rights under the UPPs.

20.50 Moreover, such a requirement would impose little or no additional compliance burden on agencies and organisations, given that they are already required to notify individuals of various matters, and this requirement is merely explanatory of the existing options available to individuals who have a complaint. In other words, it does not require any new avenues of complaint to be made available.

Proposal 20–2 The proposed 'Specific Notification' principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

(a) fact and circumstances of collection (for example, how, when and from where the information was collected);

(b) identity and contact details of the agency or organisation;

(c) fact that the individual is able to gain access to the information;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and

44 See Proposal 15–1.

(g) avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

This requirement should only apply: (1) in circumstances where a reasonable person would expect to be notified; (2) except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and (3) subject to any other relevant exceptions.

Proposal 20–3 The Office of the Privacy Commissioner should provide guidance to assist agencies and organisations in ensuring that individuals are properly informed of the persons to whom their personal information is likely to be disclosed.

Proposal 20–4 An agency should be required to notify an individual of the matters listed in the proposed 'Specific Notification' principle, except to the extent that the agency is required or specifically authorised by or under law not to make the individual aware of such matters.

Notification where information collected from a third party

Background

20.51 In IP 31, the ALRC asked whether the notification obligations imposed on organisations, agencies or both, at or soon after collection, should apply irrespective of the source of personal information.[45] This gave rise to two specific questions.

20.52 First, should an individual be notified of the source of personal information received by an agency or organisation, where that information was provided by a third party—that is, someone other than the individual in question? Neither the IPPs nor the NPPs impose such a requirement.

20.53 Secondly, which third parties should be covered by NPP 1.5 (or the equivalent of this provision in the proposed UPPs)? In 2005, the OPC recommended that consideration be given to amending NPP 1.5 to make it clear that an organisation's notification obligations under that principle apply when collecting personal information indirectly, from any source.[46] This recommendation arose because of some ambiguity in the wording of NPP 1.5, which imposes obligations on an organisation

45 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–5.

46 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 76. This is consistent with Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003).

when it collects information, not from the individual concerned, but from 'someone else'. There is uncertainty about whether 'someone else' applies to collection from some specific types of publicly available sources of information such as newspapers, books, and court reports.[47]

Submissions and consultations

Notification of source of information collected from a third party

20.54 Some stakeholders supported a requirement that individuals be notified of the source of personal information collected where that information was not collected directly from the individual.[48]

20.55 Others expressed some reservation about such an amendment. The Institute of Mercantile Agents argued that such a requirement could, in some circumstances, be dangerous in that this may put the source of the information at risk of 'domestic violence and other forms of repercussion'.[49] The National Health and Medical Research Council also expressed this concern, arguing that the notification requirement should be waived where there is a 'serious threat to the life or health of any individual'.[50] Similarly, the Office of the Information Commissioner Northern Territory stated that any such requirement should be 'subject to recognition that there will be circumstances in which the identity of the source should be protected'.[51]

20.56 United Medical Protection Ltd submitted that such a notification requirement is unnecessary because it 'will either occur as a matter of necessity or be obvious on its face'.[52]

Scope of third party notification obligations

20.57 A number of stakeholders submitted that agencies and organisations should be required to notify individuals of the collection of personal information irrespective of the source of personal information.[53] It was noted that the contrary position would

---

47 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 262. Issues relating to publicly available sources in an electronic form are discussed in Ch 8.

48 See Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

49 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

50 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

51 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

52 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

53 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

create 'a risk that the intention of ensuring individuals were aware who was collecting their information and its use could be circumvented by using third party information providers'.[54]

20.58 Some stakeholders argued that the notification obligations in NPP 1 should not arise:

- where the information in question is 'generally available', such as an address obtained from the telephone book;[55]
- where information is collected solely for the purposes of underwriting insurance, because to impose the NPP 1 obligations in these circumstances would be 'cumbersome, difficult and costly … with little or no benefit to the individual concerned';[56] and
- unless it is 'practicable and appropriate' to notify the individual concerned, bearing in mind that there are 'many circumstances', particularly in the area of health care and research, where it is not practicable or appropriate.[57]

20.59 Other stakeholders opposed any change to the current arrangements. The Institute of Mercantile Agents resisted this addition to an already 'excessive' compliance burden, arguing that it would cause 'delays and costs [that would be] on charged to … the consumer'.[58] The Australian Federal Police (AFP) stated that such an amendment would be unnecessary, assuming it applied to the AFP, given the high quality of its record-keeping methods.[59]

ALRC's view

Notification of source of information collected from a third party

20.60 The ALRC believes it is generally appropriate that, where an agency or organisation receives personal information about an individual from a source other than the individual, it should notify the individual of the source of that information.[60] This provides an important mechanism for an individual to retain some control over the quality, among other things, of personal information about the individual that is handled by agencies and organisations.

---

54 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

55 AAMI, *Submission PR 147,* 29 January 2007. However, the contrary view was expressed in Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

56 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007. See also AXA, *Submission PR 119,* 15 January 2007.

57 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

58 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

59 Australian Federal Police, *Submission PR 186,* 9 February 2007.

60 As explained later in this chapter, the ALRC believes that this general obligation should not apply where an agency or organisation has received unsolicited personal information and it chooses immediately to destroy it.

20.61 There is some precedent for this in other jurisdictions. For example, German law provides that a data subject should be provided with information about stored data concerning him or her, including any reference to the origin of the data.[61]

20.62 The second question is whether this requirement should be subject to any qualifications or exceptions. Currently, NPP 1.5 already provides that the existing notification requirements apply, 'except to the extent that making the individual aware of the [relevant] matters would pose a serious threat to the life or health of any individual'. The ALRC proposes that this exception be retained.[62]

20.63 Moreover, agencies (but not organisations) would also be subject to the additional exception in Proposal 20–4 below. That is, an agency would be required to notify an individual of the source of personal information received from a third party, except to the extent it is required or specifically authorised by or under law not to make the individual aware of such matters.

Scope of third party notification obligations

20.64 The ALRC agrees with the general proposition, expressed by a number of stakeholders, that the specific notification obligations should apply to a broad range of third parties that provide personal information to agencies and organisations. The alternative position would encourage those agencies and organisations that do not wish to comply with notification requirements to collect personal information as much as possible from third parties.

20.65 This would be undesirable for two main reasons. First, it would be likely to jeopardise the quality of the personal information collected because a source, other than the original source, is less likely to be able to keep the information accurate and up-to-date. Secondly, it detracts from the level of control that an individual can exert over his or her personal information, because the individual is less likely to know of the collection and the attendant rights that flow from this.

20.66 Therefore, the ALRC's view is that where an agency or organisation collects personal information from someone other than the individual concerned, and the individual requests that the agency or organisation inform him or her of the source of this information, the agency or organisation should be required take reasonable steps to ensure that the individual is or has been made aware of the source of the information.

20.67 Although this is the ALRC's general position, clearly it would be overly burdensome to require agencies and organisations to comply with all of the requirements in the privacy principles, and particularly the specific notification

---

61 See *Federal Data Protection Act 1990* (Germany) ss 19(1), 34(1).

62 See Proposals 20–2 and 20–5 and, generally, Ch 18.

requirements, in respect of *all* personal information that they receive. Take the following example. It is common for agencies and organisations to pay a fee to a business that provides press clippings in relation to issues that may be of interest or otherwise relevant to the agency or organisation. Those press clippings are likely to contain a considerable amount of personal information. After they are received, the press clippings are often logged and filed in a central database in case they become useful at a later data. In these circumstances, it would be a huge administrative and financial burden for an agency or organisation to comply with the notification and other requirements with respect to every piece of personal information contained in the press clippings.

20.68 The ALRC believes there is a threefold solution to this problem. First, the ALRC proposes that, where an agency or organisation receives unsolicited personal information, it should have a choice between either destroying the personal information, or retaining it but then complying with the requirements of the UPPs.[63] This would cover a considerable amount of the information in this area that ought not to import notification and other requirements.

20.69 Secondly, the ALRC shares the OPC's view that an agency or organisation should be required to comply with the specific notification requirements only in circumstances where a reasonable person would expect to be notified. The addition of an objective test along these lines would help remove ambiguity as to the obligations on an agency or organisation when it has merely received personal information from a public source, and notification would serve no useful purpose for the individual concerned. It would also mean that bodies involved in, for example, law enforcement would not be required to fulfil specific notification requirements if, in complying with these requirements, the body would undermine their lawful reason for collecting the personal information.

20.70 Thirdly, the OPC should provide guidance as to the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information about the individual from a third party. By using the mechanism of guidance—as distinct from a more prescriptive legislative solution—the UPPs will remain more flexible and better able to accommodate a wide range of circumstances.[64] The cost of such an approach is, undoubtedly, a loss of some measure of regulatory certainty. Nevertheless, the ALRC believes that, on balance, this is preferable to attempting to particularise in the *Privacy Act* the requirements relating to every conceivable source of personal information.

---

63 See Proposal 18–2.

64 See also Proposal 15–1.

Proposal 20–5 (a) The proposed 'Specific Notification' principle should provide that where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of:

(i) the matters listed in Proposal 20–2; and

(ii) on request by the individual, the source of the information.

(b) This requirement should only apply:

(i) in circumstances where a reasonable person would expect to be notified;

(ii) except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and

(iii) in the case of an agency, except to the extent that it is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.

Proposal 20–6 The Office of the Privacy Commissioner should provide guidance on the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information about the individual from a source other than the individual concerned.

Meaning of 'reasonable steps'

20.71 When an organisation collects personal information from the individual concerned or a third party, the organisation is required to take 'reasonable steps' to ensure that the individual from whom the organisation collects the information is aware of certain specified matters.[65] There is some uncertainty over what is meant by the term 'reasonable steps' and, especially, whether an organisation may legitimately conclude that, in certain circumstances, it would be reasonable to take no steps. For example, the OPC Review stated that it would be reasonable to take no steps to provide notice where significant cost or difficulty is involved in contacting a third party whose information

65 See *Privacy Act 1988* (Cth) sch 3, NPP 1.3 and NPP 1.5.

has been collected incidentally, or in many circumstances where the information is collected from a public source.[66]

20.72 Previously, it has been recommended that the legislation be amended to make clear that that there are situations in which the reasonable steps an organisation might take to provide notice to an individual may equate to no steps.[67] The ALRC asked whether such an amendment would be desirable.[68]

Submissions and consultations

20.73 A large number of stakeholders supported such an amendment.[69] Some provided examples to illustrate their view that it is sometimes reasonable to take no steps to inform the individual of the matters specified in NPP 1.3. These include the following:

- where an organisation receives information from a related body corporate, especially if the individual would reasonably expect the information to be disclosed in this way;[70]
- where an insurer collects information about the medical history of family members of an individual client;[71]
- disclosing to an individual that information about the individual has been collected as part of an alternative dispute resolution scheme may put at risk the safety of third parties;[72]
- in the context of 'family, social or medical history-taking';[73] and

66 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 260.

67 Ibid, rec 75; R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 179.

68 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–2.

69 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; ANZ, *Submission PR 173,* 6 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007.

70 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A similar example is given where personal information is disclosed to a contracted service provider: Law Council of Australia, *Submission PR 177,* 8 February 2007.

71 AXA, *Submission PR 119,* 15 January 2007.

72 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

73 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007. See also the more detailed discussion of this issue in Part H.

- in the course of an investigation into possible wrongdoing (where this investigation is not covered by the law enforcement exception).[74]

20.74 While reiterating its view that such an amendment should be made, the OPC also stated that a 'reasonable person' test should be included to help an organisation (or agency) determine what steps should be taken to make individuals aware of matters relating to the collection of their personal information.[75]

20.75 One submission stated that the solution to this problem may be to require specific notification by the data collector, 'with a conditional exception where the data [collector] could establish that at least the typical data subject had been made aware by other means'. Moreover, it may be appropriate to apply differing requirements 'depending on how the data [are] collected, with the default position being that notice is required unless an exemption is provided'.[76]

20.76 Some stakeholders submitted that no amendment was needed to the 'reasonable steps' requirement. The Australian Privacy Foundation submitted that an amendment such as that proposed 'would invite self serving interpretation to avoid giving notice even where it was both reasonable and practicable'.[77] DLA Phillips Fox submitted that NPP 1.3 already sets out 'an objective test of what is reasonable in the circumstances'.[78]

20.77 Others suggested that the solution might be simply to make the OPC more involved in the specific notification process. Telstra suggested that the OPC should issue detailed guidelines on what steps are required to provide notification in various circumstances.[79] The Law Council of Australia suggested that the solution may be to make clear that, if a person relies on advice from the OPC that no steps are required, then this should be a full defence if a complaint is later made about the person.[80]

ALRC's view

20.78 As noted above, concerns about the ambiguous meaning of 'reasonable steps' (as the term is used in NPP 1.3 and 1.5) overlaps with the question, dealt with above, whether specific notification requirements should apply with respect to personal information collected by an agency or organisation from *any* source. Again, to some extent, the problem is a lack of definitive guidance on the meaning of the term

---

74 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

75 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

76 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

77 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

78 DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

79 Telstra, *Submission PR 185,* 9 February 2007.

80 Law Council of Australia, *Submission PR 177,* 8 February 2007.

'reasonable steps'. For example, if there were an accumulated body of jurisprudence on this issue, this may provide greater confidence to agencies and organisations that collect personal information.

20.79 A number of stakeholders identified that real confusion is caused by the fact that the term 'reasonable steps' implies that at least some *active* steps must be taken by the data collector. This is despite the fact that, in certain circumstances, logic dictates that a data collector need not do anything to notify an individual. On the other hand, the fact that an agency or organisation need only take reasonable steps is, in most situations, an important and useful qualification to the specific notification obligations.

20.80 The ALRC is of the view that the best solution to this problem involves two limbs. First, the OPC should issue guidance on the meaning of the term 'reasonable steps' in this context. This would go a long way to removing the ambiguity.

20.81 Secondly, the ALRC believes that any remaining ambiguity in this area would be removed if Proposal 20–5 is adopted. That is, the ALRC believes that the 'Specific Notification' principle in the proposed UPPs should provide that, where an agency or organisation receives personal information from a third party, it need only comply with the relevant notification requirements in circumstances where a reasonable person would expect to be notified.

Proposal 20–7 The Office of the Privacy Commissioner should provide guidance on the meaning of the term 'reasonable steps' in the context of an agency's or organisation's obligations to fulfil its notification requirements under the proposed 'Specific Notification' principle.

Summary of proposed 'Specific Notification' principle

20.82 In summary, the ALRC's view is that the third principle in the proposed UPPs should be called 'Specific Notification'. It should appear as follows.

UPP 3. Specific Notification

3.1 At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

(a) fact and circumstances of collection (for example, how, when and from where the information was collected);

(b) identity and contact details of the agency or organisation;

(c) fact that the individual is able to gain access to the information;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and

(g) avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

3.2 Where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of:

(a) the matters listed in UPP 3.1 above; and

(b) the source of the information, if requested by the individual.

3.3 An agency or organisation must comply with the obligations in UPPs 3.1 and 3.2:

(a) in circumstances where a reasonable person would expect to be notified; and

(b) except to the extent that:

(i) making the individual aware of these matters would pose a serious threat to the life or health of any individual;

(ii) in the case of an agency, the agency is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.

21. Openness

Contents

Introduction 651
Current coverage by IPPs and NPPs 652
Separate 'Openness' principle? 652
ALRC's view 653
Regulatory structure: 'Privacy Policies' 654
ALRC's view 655
Matters to be included in a Privacy Policy 656
Submissions and consultations 656
ALRC's view 658
Availability of Privacy Policy 660
Submissions and consultations 660
ALRC's view 661
Short form privacy notices 662
Background 662
Submissions and consultations 663
ALRC's view 664
Summary of proposed 'Openness' principle 664

Introduction

21.1 The *Privacy Act 1988* (Cth) requires agencies and organisations to make available a document that sets out their policies relating to the management of personal information. These are referred to as 'openness' requirements, and should be contrasted with the 'specific notification' requirements in the Act. As explained in Chapter 20, the specific notification requirements differ in that they oblige agencies and organisations to notify each individual whose personal information is collected of particular matters that are specific to the individual and the personal information in question.

21.2 This chapter covers the following main issues. First, it considers the structure of the 'Openness' principle in the proposed Unified Privacy Principles (UPPs). Secondly, the ALRC proposes a system whereby agencies and organisations create a 'Privacy Policy', setting out their polices on the management of personal information and how personal information is collected, held, used and disclosed. Thirdly, the chapter considers how Privacy Policies should be made available. Finally, the ALRC addresses the issue of 'short form' privacy notices.

Current coverage by IPPs and NPPs

21.3 The Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) both set out openness requirements. IPP 5.1 provides that a record-keeper, in possession or control of records containing personal information, must take reasonable steps to enable any person to ascertain:

- whether the record-keeper has possession or control of any records that contain personal information; and
- if so, the nature of the information, the main purposes for which it is used and how to gain access to the record containing the information.

21.4 The record-keeper does not need to comply with IPP 5.1 if required or authorised so to act by a Commonwealth law that provides for access to documents.[1] A record-keeper is also required to maintain a record setting out: the nature of the records of personal information it keeps; the purpose for which each type of record is kept; the classes of individuals about whom records are kept; the period of retention; who is entitled to access and upon what conditions; and how persons can access the information. The record-keeper is to make the record setting out the above information available for public inspection, and is to give the Privacy Commissioner a copy of the record in June each year.[2]

21.5 NPP 5 provides that an organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it. On request, an organisation must take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Separate 'Openness' principle?

21.6 There are obvious parallels between the openness principles in the *Privacy Act*,[3] and the specific notification requirements in the privacy principles.[4] In particular, all of these provisions require notice to be given to individuals in relation to the information-handling practices of the relevant agency or organisation. The main difference between these principles is that the openness principles (IPP 5 and NPP 5) set out the requirements to provide notification of the *general* practices of an agency or organisation in its management of personal information, whereas IPP 2 and NPP 1.3

---

1 The two main pieces of Commonwealth legislation providing for access to documents are the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth). Access to personal information is dealt with in Chs 12 (personal information held by agencies) and 26 (personal information held by organisations).

2 This is discussed further in Part F of this Discussion Paper.

3 See *Privacy Act 1988* (Cth) s 14, IPP 5; sch 3, NPP 5.

4 See Ibid s 14, IPP 2; sch 3, NPP 1.3

require an agency or organisation to notify an individual of how it will, or is likely to, deal with that individual's particular personal information.

21.7 The following question arises: should the requirements relating to openness be dealt with in the same privacy principle that sets out the specific notification requirements? As noted in Chapter 20, some stakeholders suggested linking the notification requirement into a single privacy principle covering all of the issues (though not necessarily all of the content) currently dealt with in IPPs 2 and 5 and NPPs 1.3 and 5.[5]

21.8 Some stakeholders specifically suggested an 'awareness principle', which would cover 'notification requirements at the time of collection and more general information provision'. It was stated that attention should be given to the respective roles of proactive notice and obligations to respond to inquiries.[6]

ALRC's view

21.9 The ALRC acknowledges that the current openness principles (IPP 5 and NPP 5) cover similar ground to the current, and proposed, specific notification principles (IPP 2 and NPP 1.3). Nevertheless, there are also conceptual differences between these principles.

21.10 As explained in Chapter 20, the openness principle requires notification of the general practices of an agency or organisation relating to the handling of *any* personal information, whereas IPP 2 and NPP 1.3 require notification of how an agency or organisation will handle an individual's *particular* personal information. Explanation as to how an agency or organisation will deal with particular personal information that it has already collected from an individual is of assistance to an individual in that, for example, it may encourage the individual to access this particular personal information to determine whether it is accurate.

21.11 Explanation as to how an agency or organisation deals with personal information generally will assist the individual in different ways. For example, it may help an individual decide, before any personal information collection has occurred, whether to transact with the relevant agency or organisation. Such an explanation is also useful for the regulatory system more generally. It would allow, for instance, the Office of the Privacy Commissioner (OPC) to monitor an agency's or organisation's

---

5 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

6 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

compliance with the *Privacy Act* and also to recommend changes to the personal information management practices of the agency or organisation.[7]

21.12 For these reasons, the ALRC's view is that the requirements on an agency or organisation to operate openly and transparently by providing general notice of how it manages personal information should be dealt with in a discrete principle in the proposed UPPs.[8]

Regulatory structure: 'Privacy Policies'

21.13 In structuring this privacy principle, it is necessary to determine how to ensure that agencies and organisations comply with the general goals of openness and transparency. The current regulatory mechanism applicable to *agencies* requires them to:

- maintain a record setting out a number of matters relating to the agency's handling of personal information;[9] and
- make the record available for inspection by the public and give a copy annually to the OPC, which uses this to create the Personal Information Digest.[10]

21.14 Strong concern has been expressed to the ALRC that this system is not operating effectively.[11] Some stakeholders suggested that the Personal Information Digest was of limited utility and the information could be better disseminated in other ways.[12] For example, the Australian Federal Police suggested that this information could be made available 'through self publishing on agency websites in line with guidelines issued by the Privacy Commissioner'.[13]

21.15 The present regulatory mechanism for ensuring transparency in the management of personal information by *organisations* requires them to:

- produce a document, available to anyone on request, which sets out the organisation's privacy policy;

---

7 This is discussed in greater detail in Part F, and especially Ch 42.
8 See Proposal 21–1 below.
9 See *Privacy Act 1988* (Cth) s 14, IPP 5.3.
10 See Ibid s 14, IPP 5.4. See also s 27(1)(g).
11 The concerns about the Personal Information Digest system are described in detail in Ch 44.
12 See Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
13 Australian Federal Police, *Submission PR 186,* 9 February 2007.

- take reasonable steps, on request, to inform a person, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.[14]

21.16 In summary, agencies and organisations are required to produce some kind of document setting out their personal information management practices. The matters that must be included in this document vary depending on whether the entity in question is bound by the IPPs or the NPPs. The additional requirement that applies to entities that are bound by the IPPs is that they must furnish a copy of this document to the OPC for inclusion in the Personal Information Digest. A question arises whether these requirements should be consolidated and simplified under the proposed UPPs.

ALRC's view

21.17 The ALRC's view is that the openness requirements, currently located in the IPPs and NPPs, should be consolidated and simplified in the proposed UPPs. The ALRC believes that an agency or organisation should be required to produce a document setting out how it manages personal information and how personal information is collected, held, used and disclosed by it. As noted earlier, this document is referred to in this Discussion Paper as a 'Privacy Policy'.

21.18 The creation of a Privacy Policy could serve a number of useful purposes, including to:

- encourage agencies and organisations to consider how the UPPs apply to their activities so that they can structure their operations to comply with the UPPs;

- allow an individual to become informed, even before he or she enters into a transaction with an agency or organisation, about the agency's or organisation's personal information-handling practices. This will help the individual to make a more informed choice on matters such as whether he or she wishes to transact with the agency or organisation in question; and

- aid in the process of auditing to be carried out by the OPC.[15]

21.19 As noted below, there is some precedent in New South Wales law for a regulatory mechanism along the lines of the ALRC's proposal.[16] The specific matters than an agency or organisation would be required to include in its Privacy Policy, and other associated issues, are discussed below. It should be noted, however, that this

---

14 See *Privacy Act 1988* (Cth) sch 3, NPP 5.

15 The OPC's audit function is discussed in Part F.

16 See *Privacy and Personal Information Protection Act 1998* (NSW) s 33, which requires New South Wales public sector agencies to create and implement 'Privacy Management Plans'.

proposal would ease the compliance burden on agencies because they would no longer be required to submit a document to the OPC for the purposes of the Personal Information Digest.

Proposal 21–1 The proposed Unified Privacy Principles should contain a principle called 'Openness' that sets out the requirements on an agency or organisation to operate openly and transparently by providing general notification in a Privacy Policy of how it manages personal information and how personal information is collected, held, used and disclosed by it.

Matters to be included in a Privacy Policy

21.20 The openness requirements applicable to agencies and organisations differ, in that NPP 5 imposes a general obligation on an organisation to maintain a document setting out its policies on the management of personal information, whereas IPP 5 takes a more prescriptive approach. As noted above, IPP 5 lists the specific matters that must be included in the record summarising how the agency manages personal information.

21.21 Assuming that the ALRC's proposal to require agencies and organisations to produce Privacy Policies is accepted, it is necessary to consider whether to set out general or prescriptive obligations. If a more prescriptive approach is preferred, a further question arises as to what matters the openness principle should specify as being necessary to reveal.[17]

Submissions and consultations

21.22 Given that IPP 5 is already prescriptive as to the matters that must be recorded by agencies, stakeholders generally focused on whether it is preferable to be more prescriptive as to the openness obligations applicable to *organisations*. The OPC submitted that 'the obligations imposed by NPP 5 require more specificity to remain relevant and effective', but this should not allow the principle to become too prescriptive because this would run contrary to the regulatory framework of the Act.[18] Some other stakeholders also noted that greater guidance could be provided in guidelines, as distinct from primary legislation.[19]

21.23 Some stakeholders supported more prescriptive requirements, and suggested that the following requirements should be incorporated:

---

17 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–20.

18 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

19 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

- The openness obligations on agencies and organisations should be to: (1) inform individuals how to access the agency's or organisation's information management policies; (2) provide a specific response to any request from an individual for the 'sort' of information held about the individual; and (3) comply with the requirements currently listed in NPP 5.2—that is, to let individuals know the sort of personal information an organisation or agency holds; the purposes for which it is held; and how it collects, holds, uses and discloses the information.[20]

- The OPC should be given the discretion to 'require organisations to publish further information about particular personal information handling projects'.[21]

- Agencies and organisations should make available the 'details of the information systems used to maintain relevant databases' as this would allow individuals to assess the security and other qualities of the information-handling system.[22]

- Customers should be notified of 'material changes to [the organisation's] privacy practices'. This obligation would apply, for instance, where an organisation wishes to use or disclose personal information already collected for an expanded or new secondary purpose.[23]

21.24 Other stakeholders opposed taking a prescriptive approach to the openness obligations. A number of stakeholders argued that the current obligations were sufficiently clear.[24] Some stakeholders argued that a prescriptive approach would hamper the ability of organisations to tailor privacy policies to customers' needs and it may contribute to overly long privacy notices.[25] AAMI stated that requiring organisations to submit their privacy documents to the OPC 'would be unlikely to add any real value'.[26]

21.25 DLA Phillips Fox argued that the less onerous requirements in NPP 5, as compared with IPP 5, reflect that personal information held in the private sector is

---

20 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

21 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

22 W Caelli, *Submission PR 99,* 15 January 2007.

23 Microsoft Australia, *Submission PR 113,* 15 January 2007.

24 Law Council of Australia, *Submission PR 177,* 8 February 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

25 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

26 AAMI, *Submission PR 147,* 29 January 2007. See also Investment and Financial Services Association, *Submission PR 122,* 15 January 2007.

more likely to have been voluntarily provided by the individual concerned than that held by government agencies.[27] It was also submitted that NPP 5 and IPP 5 should not be compared in isolation from the other privacy principles. The National Australia Bank and MLC argued that the requirements in the related principle, NPP 1.3, are more onerous than the equivalent IPP 2.[28]

ALRC's view

21.26 The ALRC believes that an appropriate balance can be struck between the objective of providing greater clarity and certainty as to the openness requirements on agencies and organisations, and the competing objective of setting out obligations in a general way. That is, by stressing the goals to be achieved while allowing flexibility to agencies and organisations in how they achieve these goals.[29] The best way to achieve such a balance is to provide enough detail in the relevant privacy principle to ensure that the obligations are clear, and then for the OPC to provide guidance as to the more detailed requirements. This approach aims to reconcile the differing views of stakeholders on this issue.

21.27 As to the specific matters that should be listed in a Privacy Policy, there are some requirements that are common to the IPPs and NPPs. That is, both sets of privacy principles require disclosure of the sort of personal information that is held, and the purposes for which personal information is held.

21.28 There is then a divergence between the NPPs and the IPPs. NPP 5 simply requires disclosure of the organisation's policies on the management of personal information, and how the personal information is collected, held, used and disclosed. On the other hand, IPP 5 requires the following additional categories of information to be made available: (1) the classes of individuals about whom records are kept; (2) the period for which each type of record is kept; (3) the persons who can access personal information and the conditions under which they can access it; and (4) the steps an individual may take to gain access to personal information.

21.29 There seems general consensus that the categories of information required to be disclosed by *both* the IPPs and NPPs should be retained in the proposed UPPs. Additionally, the ALRC believes that the following items should also be included in a Privacy Policy:

- A summary of the avenues of complaint available to individuals in the event that they have a privacy complaint. Although the ALRC proposes that this should also be included in the specific notification obligations,[30] it would be of

---

27 DLA Phillips Fox, *Submission PR 111,* 15 January 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

28 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

29 See Proposal 15–1 and accompanying text.

30 See Proposal 20–3.

assistance to make this information available in the Privacy Policy as well, because the Privacy Policy is more likely to be generally available. As to the details of this requirement, the ALRC believes that an agency or organisation should generally nominate an internal dispute resolution contact and identify whether it is part of an external dispute resolution scheme (such as the Telecommunications Industry Ombudsman or Banking and Financial Services Ombudsman).[31] The ALRC believes, however, that these details should be provided in guidance from the OPC, rather than being incorporated in the proposed 'Openness' principle itself.

- The steps individuals may take to gain access to personal information held by the entity in question. This would be a minor addition to the Privacy Policy and would help individuals in exercising their access and correction rights.

- The remaining items listed in IPP 5.3 that are not explicitly listed in NPP 5—namely: (1) the types of individual about whom records are kept; (2) the period for which each type of record is kept; and (3) the persons, other than the individual, who can access personal information and the conditions under which they can access it. The consolidation of these requirements in the proposed UPPs would help to ensure that the privacy principles in the Act are generally applicable, and that individuals are able to inform themselves adequately about the personal information management practices of agencies and organisations. Moreover, the ALRC believes that, as organisations will have to inform themselves about these matters in order to comply with other privacy principles, it will not be unreasonably onerous for them to list this information in their Privacy Policy.

Proposal 21–2 The Privacy Policy in the proposed 'Openness' principle should set out an agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;

31 A similar obligation, in relation to internal dispute resolution, is provided for in *Privacy and Personal Information Protection Act 1998* (NSW) s 33(2)(c).

(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation;

(e) the types of individuals about whom records are kept;

(f) the period for which each type of record is kept; and

(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.

Proposal 21–3 The Office of the Privacy Commissioner should issue guidance on how agencies and organisations can comply with their obligations in the proposed 'Openness' principle to produce and make available a Privacy Policy.

Availability of Privacy Policy

21.30 The NPPs and IPPs differ in that IPP 5 requires a record-keeper to take reasonable steps to enable an individual to ascertain specified matters irrespective of whether the individual has made a request, whereas the corresponding obligation in NPP 5 only applies to an organisation following a request by an individual. The ALRC asked whether the better model, in relation to this issue, is provided by NPP 5 or IPP 5.[32]

Submissions and consultations

21.31 Some stakeholders submitted that the requirements to make certain information available should apply irrespective of whether an individual has requested that information.[33] The Office of the Victorian Privacy Commissioner stated that general details about an organisation's information-handling practices should be readily available even without an individual making a request, but that more detailed information should be the subject of a request.[34] Another stakeholder submitted that, where a request is denied, this should be accompanied by reasons that can be evaluated by the OPC.[35]

32 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–21.

33 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; W Caelli, *Submission PR 99,* 15 January 2007.

34 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

35 W Caelli, *Submission PR 99,* 15 January 2007.

21.32 Other stakeholders suggested that an individual's request is the appropriate trigger for at least some notification requirements.[36] The OPC submitted that, if the notification requirements are otherwise enhanced, the provision of the specific 'sort' or 'types' of information held about an individual should be triggered by the individual's request.[37] AAMI argued that, provided individuals are made aware of their right to request the relevant information, it is more appropriate that an individual's request trigger this obligation.[38]

21.33 The Australian Bankers' Association was concerned about the amount of information that must already be made available to consumers. It argued that, if the obligations were triggered without an individual's request, customers could be over-burdened with paper information.[39] The Australian Government Department of Health and Ageing also favoured extending the request-based approach in the NPPs to agencies, arguing that this would be more cost effective and practically useful for individuals.[40]

ALRC's view

21.34 The ALRC's view is that agencies and organisations should be required to provide an individual with a physical or hard copy of its Privacy Policy only when an individual requests it. This is consistent with the view of a large number of stakeholders. To require the provision of a physical or hard copy without a request would overburden agencies and organisations. It would also be of limited assistance to individuals, who already receive a large amount of general disclosure information in their transactions with government and the private sector.

21.35 Consequently, the ALRC believes that the better approach is for agencies and organisations to make their Privacy Policy readily available electronically—for example, on their website, if they have one. If, however, this option is unavailable or, for any reason, an individual cannot or does not wish to obtain the Privacy Policy in an electronic form and requests a hard copy, the agency or organisation should provide one. If an individual requests a copy of an agency's or organisation's Privacy Policy, he or she should not be charged a fee for this information. This reflects the underlying

---

36 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

37 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

38 AAMI, *Submission PR 147,* 29 January 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AXA, *Submission PR 119,* 15 January 2007.

39 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

40 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

principle, discussed in Chapter 29, that an individual should not be unreasonably disadvantaged for seeking to assert or enjoy his or her privacy rights.

Proposal 21–4 An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the proposed 'Openness' principle, available without charge to an individual: (a) electronically (for example, on its website, if it possesses one); and (b) in hard copy, on request.

Short form privacy notices

Background

21.36 A short form privacy notice is, simply, a summary of an agency's or organisation's practices for the management of personal information. By creating a short form privacy notice, an agency or organisation will not necessarily fulfil its obligations under the openness principle. They are useful, however, because they can help individuals quickly understand broadly how the agency or organisation in question handles personal information.

21.37 A question arises whether specific provision should be made in the *Privacy Act* for short form privacy notices.[41] The obligation under NPP 5 for an organisation to maintain a document setting out its policies on the management of personal information has been described as 'somewhat vague about what it requires organisations to do'.[42] There is a question whether the requirement should make clear whether short form privacy notices are included.

21.38 In 2005, the OPC recommended that the Australian Government consider amending NPP 5.1 to provide for short form privacy notices. This could also clarify the obligations on organisations to provide notice, and clarify the links between NPP 1.3, which imposes an obligation to take reasonable steps to ensure an individual is aware of specified matters at or before the time of collection of personal information, and NPP 5.1.[43]

21.39 The OPC said that short form notices 'would improve the quality of an organisation's communication with its customers', and further:

> A long privacy notice may not fulfil its purpose of informing a consumer because the consumer may be overwhelmed and confused … The Office's Community Attitudes Survey reports international research that shows that people do not necessarily read privacy notices, partly because they are too long and complex.

---

41 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–22.

42 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

43 Ibid, rec 19.

> Longer privacy notices have come about partly as a result of organisations' uncertainty as to the distinction between the primary and secondary purposes of collection and their attempt to avoid 'bundling' consent to a number of purposes of collection … There could be provision for short form notices, followed by a longer notice that includes all the information required by NPPs 1.3 and 1.5.[44]

21.40 The OPC indicated that it would encourage the development of short form privacy notices. It said it would play a more active role in assisting businesses develop their notices.[45]

Submissions and consultations

21.41 A number of stakeholders supported the privacy principles making provision for short form privacy notices.[46] The OPC noted:

> Providing greater detail at the point of collection may, in fact, be counter productive as research shows that many people do not read or do not understand lengthy privacy notices or policies.[47]

21.42 The OPC argued that such a requirement 'may not be overly burdensome and may in fact assist agencies and organisations in promoting consumer confidence'.[48] A number of stakeholders noted that they already provide short form privacy notices.[49]

21.43 Some stakeholders argued that providing short form privacy notices does not obviate the need also to provide more detailed information. In other words, 'layered' privacy notices—involving a series of privacy notices that provide differing levels of detail—can be helpful.[50] The OPC submitted that 'more detailed information regarding the personal information management policies of an organisation or agency' should be made available in a separate document to individuals on request.[51]

---

44 Ibid, 91–92.

45 Ibid, rec 20. In August 2006, the OPC launched its layered privacy policy notice. See Office of the Privacy Commissioner, 'Release of Privacy Impact Assessment Guide and Layered Privacy Policy' (Press Release, 29 August 2006) and Office of the Privacy Commissioner, *Privacy Policy* (2006).

46 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

47 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

48 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

49 AAMI, *Submission PR 147,* 29 January 2007; DLA Phillips Fox, *Submission PR 111,* 15 January 2007.

50 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

51 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

21.44 On the other hand, while noting that short form privacy notices may be beneficial in certain circumstances, some stakeholders submitted that they should not be mandatory.[52]

ALRC's view

21.45 The ALRC agrees that short form privacy notices are of considerable assistance in communicating the basic outline of the personal information management practices of agencies and organisations. Any provision for, or encouragement of, short form privacy notices, however, should not be at the expense of an agency or organisation producing a detailed and comprehensive Privacy Policy, and also providing specific notification as discussed in Chapter 20.

21.46 The ALRC is, therefore, of the view that best practice by agencies and organisations is to create 'layered' privacy notices. This involves making at least two versions of a privacy notice available to individuals—a comprehensive and detailed explanation of the entity's privacy practices, and a more abbreviated summary. Both can be made available easily and cheaply in an electronic form, such as via an agency's or organisation's website.

21.47 On the other hand, given the desire to maintain a light-touch approach to the privacy principles,[53] the ALRC believes that it is more appropriate for the OPC to encourage and guide the adoption of short form privacy notices, rather than mandating them in the *Privacy Act*. This approach is consistent with the recommendation of the OPC review of the private sector provisions of the *Privacy Act*.[54]

Proposal 21–5 The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

Summary of proposed 'Openness' principle

21.48 In summary, the ALRC's view is that the fourth principle in the proposed UPPs should be called 'Openness'. It should appear as follows.

52 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
53 See Proposal 15–1.
54 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 20.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out the agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation in question;

(e) the types of individual about whom records are kept;

(f) the period for which each type of record is kept; and

(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically, for example, on its website (if it possesses one); and

(b) in hard copy, on request.

22. Use and Disclosure

Contents

Introduction 667
Current coverage by IPPs and NPPs 669
Towards a single 'Use and Disclosure' principle 670
Submissions and consultations 671
ALRC's view 672
Use and disclosure of personal information for a related secondary purpose 674
Background 674
Submissions and consultations 675
ALRC's view 677
Emergencies, disasters and threats to life or health 679
Background 679
Submissions and consultations 680
ALRC's view 683
Missing persons 685
Background 685
Submissions and consultations 686
ALRC's view 687
Disclosure of 'incidents' by insured professionals to insurers 688
Submissions and consultations 688
ALRC's view 689
Use and disclosure in other contexts 690
Where required or authorised by or under law 690
Due diligence 691
Research, health care and disclosure on compassionate grounds 693
Logging disclosures 694
Background 694
Submissions and consultations 694
ALRC's view 696
Summary of proposed 'Use and Disclosure' principle 697

Introduction

22.1 The *Privacy Act 1988* (Cth) provides that, if an agency or organisation has complied with all relevant obligations in collecting personal information and the information was collected for a lawful purpose, the agency or organisation is permitted to use or disclose the information for that lawful purpose of collection. The

Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), however, generally prohibit the use or disclosure of personal information for a purpose other than the lawful purpose for which the information was collected.[1] Nevertheless, this general prohibition is subject to certain, limited exceptions, which allow agencies and organisations to use or disclose personal information they have lawfully collected for a secondary purpose in some situations.

22.2 The main aim of the use and disclosure principles (NPP 2 and IPPs 9–11) is to restrict use and disclosure of personal information for a secondary purpose of collection. Research conducted in 2001 on behalf of the Office of the Privacy Commissioner (OPC) indicated that Australians were worried about the use of personal information for a purpose other than its original purpose. Of 1,524 people interviewed, 68% stated that this was a concern to them, 41% stated it was a great concern and 23% recorded little or no concern.[2] Similarly, 35% of complaints to the OPC under the NPPs in the financial year ending 30 June 2006 related to the use or disclosure of personal information.[3] This represented the largest single category of complaint.

22.3 The OPC has reaffirmed the importance of maintaining a distinction between the primary and secondary purposes of collection, observing that this distinction allows an individual to 'maintain … knowledge and control over when personal information may be used and disclosed'.[4] It also dismissed the suggestion that the line between primary and secondary purpose is unclear:

> Determining the primary purpose of collection should always be possible. Where an organisation collects personal information directly from the individual the context in which the information is collected will help identify the primary purpose of collection. When personal information is collected indirectly, the organisation's use of the information soon after collection is a good indication of the primary purpose of collection.[5]

22.4 Given the main aim of these privacy principles is to restrict, by way of a general prohibition, the use and disclosure of personal information for a purpose other than the primary purpose of collection, the main focus of this chapter is to determine what should be the *character* and *scope* of the exceptions to this general prohibition.

22.5 This chapter covers the following main issues. First, it considers whether the use and disclosure provisions in the IPPs and NPP should be consolidated into a single use and disclosure principle in the proposed Unified Privacy Principles (UPPs). Next, the chapter addresses a number of exceptions to the general prohibition against using or disclosing personal information for a secondary purpose. The following exceptions are

---

1 This is referred to as use or disclosure for a 'secondary purpose'.

2 Roy Morgan Research, *Privacy and the Community [prepared for Office of the Federal Privacy Commissioner]* (2001), 25.

3 See Office of the Privacy Commissioner, *Complaints and Enquiries Statistics to End of March 2007* <www.privacy.gov.au/about/complaints/index.html> at 31 July 2007.

4 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

5 Ibid.

of particular significance: use or disclosure for a related secondary purpose; use or disclosure in the event of an emergency; and where use or disclosure is required or authorised by law. Finally, the chapter considers whether agencies and organisations should be required to create a log of all disclosures of personal information that they make.

Current coverage by IPPs and NPPs

22.6 IPPs 9–11 deal with use and disclosure of personal information by agencies. IPP 9 provides that personal information may be used only for relevant purposes. IPPs 10 and 11, respectively, impose limitations on the use and disclosure of personal information. For organisations, the rules on the use and disclosure of personal information are set out in a single privacy principle, NPP 2.

22.7 NPP 2 and IPPs 10 and 11 restrict the use and disclosure of personal information for a purpose other than the primary purpose of collection. NPP 2 expressly uses the language of 'primary purpose' and 'secondary purpose' of collection. 'Secondary purpose' is defined as any purpose other than the primary purpose of collection.[6] In contrast, the IPPs do not use the language of 'primary' and 'secondary' purpose; instead, IPP 10 provides that where personal information is obtained for a *particular purpose* there are constraints on its use for *any other purpose*. There is, however, no significant difference in the concepts addressed here. Therefore, for the sake of simplicity, this Discussion Paper will refer to 'primary' and 'secondary' purposes for both the IPPs and NPPs.

22.8 A critical difference between the IPPs and NPPs is that NPP 2 contains provisions that permit use *and* disclosure of personal information for a secondary purpose, whereas the IPPs only permit *use* for a secondary purpose—that is, there is no mechanism for disclosure for a secondary purpose under IPP 11. IPP 11, however, does permit disclosure to a third party where the individual concerned is reasonably likely to have been aware, or made aware under IPP 2, that information of that kind is usually passed to that third party.

22.9 There are some important similarities between NPP 2 and IPPs 10 and 11. For example, NPP 2.1(a) and IPP 10.1(e) provide exceptions where the secondary purpose is sufficiently related to the primary purpose. Secondary purpose use and disclosure are also permitted under the IPPs and NPPs where:

- the individual consents to the use or disclosure;
- it is required or authorised by law;

---

6 'Primary purpose' is not defined in the Act but appears to relate to the functions or activities of an organisation. See *Privacy Act 1988* (Cth) sch 3, NPP 1.1.

- it is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty or to protect the public revenue; or

- there is a serious and imminent threat to the life or health of an individual.

22.10 The NPPs contain a greater number of exceptions to the general prohibition against secondary purpose use and disclosure than are set out in the IPPs. In particular, NPP 2 permits secondary purpose use or disclosure:

- for the safety of an individual, public health and public safety;

- in the preparation for, or conduct of, court or tribunal proceedings;

- for the prevention and investigation of 'seriously improper conduct';

- for direct marketing where specified criteria are met;[7]

- where the organisation reasonably believes that the use or disclosure is reasonably necessary for certain specified functions of an enforcement body; or

- of health information for research or statistics relevant to public health and safety where specified criteria are met.

22.11 In addition, unlike the IPPs, NPP 2 contains notes that indicate that NPP 2 is not intended to deter organisations from lawfully cooperating with law enforcement agencies and that an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.[8]

Towards a single 'Use and Disclosure' principle

22.12 Before considering the exceptions to the use and disclosure principle, it is first necessary to address the broader issue of how to structure the use and disclosure provisions in the privacy principles. This requires the resolution of two questions.

22.13 First, should *agencies* be subject to a single privacy principle dealing with use and disclosure? As noted above, the IPPs contain separate 'use' and 'disclosure' principles. Sometimes there is only a fine distinction between disclosure and use, and so it might be more practical for the issues to be dealt with in a single principle. Moreover, the fact that the IPPs treat use and disclosure separately differs from the NPPs and the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD

7 Direct marketing is dealt with separately in Ch 23.
8 See *Privacy Act 1988* (Cth) sch 3, NPP 2, Notes 1–3.

Guidelines), which each contain a single 'use and disclosure' principle.[9] In light of this, the ALRC asked, in Issues Paper, *Review of Privacy* (IP 31), whether it would be desirable for agencies to be subject to a single privacy principle dealing with use and disclosure.[10]

22.14 Secondly, insofar as the IPPs and NPPs impose differing use and disclosure requirements on agencies and organisations respectively, how should these differences be accommodated in a single privacy principle that applies both to agencies and organisations?

Submissions and consultations

22.15 The vast majority of stakeholders that commented on this issue argued that agencies should be subject to a single privacy principle dealing with use and disclosure. The OPC submitted that a single use and disclosure principle would

> assist in providing a consistent approach for the handling of personal information and may go some way to alleviating the confusion that surrounds the identification of whether certain activities and information handling practices are considered a 'use' or a 'disclosure' and which provisions and principles should apply.[11]

22.16 A number of other stakeholders expressed a similar view.[12] The National Health and Medical Research Council (NHMRC) noted that often 'whether an information transaction is a "use" or a "disclosure" is determined by corporate structures rather than by practical differences in information-handling practices'. Moreover, a single use and disclosure principle would not prevent stricter protections being imposed where appropriate:

> Where a higher degree of protection is required for a category of information transaction (e.g. in relation to disclosure for some purposes) it can still be provided within a single 'use and disclosure' principle.[13]

22.17 Some private sector stakeholders also favoured a single use and disclosure principle. It was submitted that where a private sector organisation must comply with the IPPs pursuant to a contract it has entered into with a public sector entity, it would

---

9 See Ibid sch 3, NPP 2 and Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 9.

10 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–6.

11 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

12 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Confidential, *Submission PR 130,* 17 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

13 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

be 'useful' for the Act to deal 'consistently with the principles relating to all dealings with personal information, including use and disclosure'.[14]

22.18 A number of stakeholders submitted that, in the event that the IPPs and NPPs are consolidated into a single set of privacy principles (the UPPs),[15] the 'use and disclosure' principle should be modelled on NPP 2 (as distinct from IPPs 9–11).[16]

22.19 Some stakeholders preferred that agencies be subject to separate use and disclosure principles. The Australian Federal Police (AFP) took the view that the current structure of the IPPs is working adequately and does not need to be changed.[17] One stakeholder stated that there remains a qualitative difference between internal use of information and its disclosure, and it would be inappropriate to restrict an agency from using personal information only to the circumstances listed in IPP 11. This stakeholder submitted that, if a single use and disclosure principle were adopted, an agency should be allowed to use or disclose the information for a purpose that is directly related to the purpose for which the information was collected, as is currently permitted by IPP 10.1(e).[18]

22.20 The Australian Government Department of Human Services submitted that separate principles align better with 'secrecy provisions' in other legislation.[19] Professor William Caelli's basis for retaining separate use and disclosure principles was that 'disclosure alone could lead to … identity theft problems … as distinct from any threats possible under agency/organisational usage alone'.[20]

22.21 Finally, some stakeholders were ambivalent about whether agencies should be subject to a single use and disclosure principle. This was either because this issue distracted from the more important question of what should be the *nature* of an agency's use and disclosure obligations,[21] or because the competing arguments were difficult to resolve and so it was preferred that the question remain open.[22]

ALRC's view

22.22 The ALRC's view is that it is desirable to move to a single use and disclosure principle that applies to agencies and organisations. This would provide a number of benefits. First, it would assist in the process of consolidating the IPPs and NPPs into a

---

14 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007. See also National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
15 See Proposal 15–2.
16 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
17 Australian Federal Police, *Submission PR 186,* 9 February 2007.
18 Confidential, *Submission PR 143,* 24 January 2007.
19 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
20 W Caelli, *Submission PR 99,* 15 January 2007.
21 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.
22 See G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

single set of privacy principles, the UPPs.[23] Secondly, it would help alleviate the problem that currently applies where organisations that are bound by the NPPs act as contracted service providers, and are contractually required to act consistently also with the IPPs.[24]

22.23 The ALRC accepts that there is a conceptual difference between 'use' and 'disclosure'. This is reflected in s 6(1) of the *Privacy Act*, which does not define the concept of disclosure, but does provide the following limited definition of 'use':

> ***use***, in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.

22.24 This difference is reflected in the dictionary definition of these terms. The *Macquarie Dictionary* defines 'use' to mean, relevantly: 'to employ for some purpose; put into service; turn to account'.[25] On the other hand, 'disclose' is defined to mean, relevantly: 'to cause to appear; allow to be seen; make known; reveal'.[26] Therefore, the conceptual difference between use and disclosure of personal information seems to lie in the fact that 'use' involves an active process of putting the information into service by the user, whereas 'disclosure' implies that the discloser merely acts as a conduit that enables information to be passed to another person.

22.25 Some stakeholders expressed concern that, if the rules dealing with use and disclosure of personal information by agencies were located in a single privacy principle, this would risk conflating the concepts of use and disclosure. The ALRC's view, however, is that such a reform could be carried out without creating any such conflation. For example, the fact that an individual, X, consented to the disclosure of his or her personal information to another person, Y, cannot logically mean that X also consented to the use of that information by a third person, Z, for an unrelated secondary purpose. This is how the NPPs, which deal with use and disclosure in a single privacy principle, already operate. In a practical sense, use and disclosure will often be dealt with identically; however, a single use and disclosure principle does not preclude use and disclosure being treated differently where appropriate.

Proposal 22–1 The proposed Unified Privacy Principles should contain a principle called 'Use and Disclosure' that sets out the requirements on agencies and organisations in respect of the use or disclosure of personal information for a purpose other than the primary purpose of collecting the information.

---

23 See Proposal 15–2.
24 See the further discussion on contracted service providers in Part C.
25 *Macquarie Dictionary* (online ed, 2005).
26 Ibid. Note that the noun 'disclosure' is defined solely with reference to the verb 'disclose'.

Use and disclosure of personal information for a related secondary purpose

Background

22.26 As noted above, under both the IPPs and NPPs, the general prohibition against the use or disclosure of personal information for a secondary purpose does not apply where that secondary purpose has the requisite connection with the primary purpose of collection. NPP 2.1(a) allows use or disclosure of personal information for a secondary purpose if the:

- individual would reasonably expect the organisation to use the information for the secondary purpose; and

- secondary purpose is related to the primary purpose of collection,[27] or, if the information in question is 'sensitive information', the secondary purpose is *directly* related to the primary purpose. The stricter test that applies in respect of sensitive information provides an added degree of protection.[28]

22.27 The IPPs also contain an exception in respect of related secondary *use* of personal information; however, there is no such exception in respect of the *disclosure* of personal information for a secondary purpose. The exception is provided in IPP 10.1(e), which requires that the secondary purpose must be 'directly related' to the primary purpose. IPP 10, however, does not impose the additional 'reasonable expectation' test that is provided in NPP 2.1(a).

22.28 In IP 31, the ALRC asked, in relation to NPP 2.1(a) and IPP 10(e), whether there should be:

- a 'direct' relationship between the secondary and primary purposes of collection before an *organisation* can use or disclose non-sensitive personal information for a secondary purpose;[29] and

- an additional requirement on an *agency* that the individual concerned would reasonably expect the agency to use the information for that other purpose.[30]

---

27 According to the OPC, this means that 'the secondary purpose must be something that arises in the context of the primary purpose': Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

28 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [342].

29 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–8.

30 See Ibid, Question 4–9.

Submissions and consultations

Connection between primary and secondary purpose: direct or indirect?

22.29 A number of stakeholders supported amending the related secondary purpose exception to bring it in line with IPP 10(e) for agencies and organisations. This would require a 'direct' relationship between the secondary and primary purposes of collection in order for an agency or organisation to avail itself of this exception by using or disclosing personal information (sensitive or non-sensitive) for a secondary purpose.[31] Some stakeholders noted that this would provide greater clarity to those subject to the principle, particularly given that it can be difficult to determine whether particular information is or is not 'sensitive'.[32] On the other hand, the Office of the Information Commissioner Northern Territory submitted that a better way to achieve clarity might be to provide examples (in the Act or by way of OPC guidance) illustrating where a relationship is direct and where it is indirect.[33]

22.30 One submission argued that a requirement of a 'direct' relationship was easier to apply than the equivalent provisions in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which require that the primary and secondary purposes to be 'compatible'.[34]

22.31 On the other hand, a number of stakeholders opposed amending the exception to require a 'direct' relationship between the secondary and primary purpose of collection for all categories of personal information. ANZ, for example, submitted that this would 'result in organisations requiring consent for the most obvious uses, that while not directly related, are expected by the customer'. It gave the following example:

> [T]he information provided in an application form for a credit card may be interpreted as being provided for the purpose of the application and the ongoing provision of the product, once approved, may be interpreted as a secondary purpose. However, the customer would expect the information collected on the application form to be used for the ongoing provision of the product for which they applied.[35]

---

31 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007.

32 Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

33 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

34 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. One stakeholder, however, suggested that the primary and secondary purposes should be 'consistent': Confidential, *Submission PR 143,* 24 January 2007.

35 ANZ, *Submission PR 173,* 6 February 2007.

22.32 The Commonwealth Scientific and Industrial Research Organisation (CSIRO) was also concerned that such an amendment 'would introduce further restrictions on public health research'. It stated:

> A too-restrictive requirement for a 'direct' relationship between the secondary and primary purpose could seriously limit the utility of a valuable resource. If existing datasets cannot be used for a new purpose because of this criterion, a new dataset may need to be created. In this situation the total cost of data collection would increase, the total burden of survey and study participation would increase and there will be a delay in realising the potential benefits of research.[36]

22.33 Veda Advantage argued that the appropriate criterion in determining whether a secondary use or disclosure should be permitted ought to be whether this would 'pose a significant risk of harm' to the individual in question.[37]

Reasonable expectation of use or disclosure

22.34 A number of stakeholders supported extending to agencies the requirement, already applicable to organisations, that the individual concerned would reasonably expect the agency to use or disclose the personal information for the secondary purpose in question.[38]

22.35 The OPC suggested that the reasonable expectation requirement is meant to be understood in a common sense way and is not overly onerous, pointing out that if an entity is unsure what would be the reasonable expectation of an individual in particular circumstances, it could simply seek the individual's consent.[39] The NHMRC supported such a requirement provided that the test is objective, rather than subjective.[40] On the other hand, there was some concern that a 'reasonable expectation' requirement is 'too vague and open to severe abuse'—particularly, by those engaging in data-mining—and this requirement should be clarified.[41]

22.36 Some stakeholders, however, opposed this condition being extended to agencies, arguing that the current provisions are adequate.[42] The Australian Government Department of Families, Community Services and Indigenous Affairs (FaCSIA) submitted that such a requirement would restrict how an agency uses personal

---

36 CSIRO, *Submission PR 176,* 6 February 2007. See also Veda Advantage, *Submission PR 163,* 31 January 2007.

37 Veda Advantage, *Submission PR 163,* 31 January 2007.

38 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

39 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

40 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

41 W Caelli, *Submission PR 99,* 15 January 2007.

42 Confidential, *Submission PR 165,* 1 February 2007; AXA, *Submission PR 119,* 15 January 2007.

information and 'could ultimately limit the extent to which an agency could assist individuals'. It gave the following example:

> FaCSIA administers a wide range of programmes to assist individuals. Any particular individual may be benefiting from a multiple number of programmes administered by FaCSIA. Where information about an individual is collected for the purposes of providing a particular programme, FaCSIA considers it important to retain the discretion to use such information for other reasonable purposes, such as to identify and notify the individual of another programme which the individual may benefit from.[43]

22.37 This view was challenged, however, by the OPC, which argued that the reform discussed here would not greatly change the status quo:

> The general policy concept behind IPP 10.1 is that people usually give personal information to an agency with a specific purpose in mind, such as receiving a benefit payment or a tax refund and they should be able to expect the information to be used for that purpose only… [The OPC] believes that IPP 10.1 already includes the concept of reasonable expectation and the addition of such provisions for agencies through the adoption of a single set of privacy principles would not represent an extra burden for agencies.[44]

ALRC's view

Connection between primary and secondary purpose: direct or indirect?

22.38 There was considerable disagreement among stakeholders as to whether the 'related purpose' exception in the use and disclosure principle should require a *direct* relationship between the secondary purpose and primary purpose in respect of both sensitive and non-sensitive personal information.

22.39 While acknowledging that such an amendment may provide some added protection against use and disclosure of an individual's personal information that is beyond the individual's reasonable expectation, the ALRC believes that the disadvantages of such an approach outweigh the potential benefits. The ALRC is concerned about two problems in particular.

22.40 First, such an approach could be very onerous on data collectors, effectively requiring them to seek consent whenever they wish to use or disclose an individual's personal information for a purpose that is not precisely 'on all fours' with the original purpose of collection. This problem is particularly prevalent where an individual is a customer of a large organisation that handles the individual's personal information for multiple products or services. As a corollary, there is little, if any, real benefit for the individual in being asked repeatedly to consent to particular uses and disclosures of his

---

43 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

44 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

or her personal information. Indeed, such a requirement might encourage organisations to seek 'bundled' consent, something that the ALRC is attempting to avoid.[45]

22.41 Secondly, there is also a concern that a direct relationship test may hamper legitimate scientific and other research. This concern is likely to be addressed, at least in part, by the more detailed provisions proposed by the ALRC to deal with the secondary use and disclosure of personal information in the health and research contexts.[46] The ALRC acknowledges, however, that such provisions will not necessarily cover all aspects of legitimate research and, if the related secondary purpose exception is too narrow, it could hamper some research carried out, especially by private sector organisations.

22.42 In conclusion, the ALRC's view is that the related secondary purpose exception in the 'Use and Disclosure' principle of the proposed UPPs should import, as its first limb, the equivalent provision in NPP 2.1(a)(i). That is, in order to avail itself of this exception, an agency or organisation should be required to show that the secondary purpose is related to the primary purpose of collection for all personal information other than sensitive information, for which a direct relationship should continue to be required.

Reasonable expectation of use or disclosure

22.43 The term 'reasonable expectation' imports an objective test of what a hypothetical reasonable individual would expect in the relevant circumstances. A significant majority of stakeholders supported, as a condition to the exercise of this exception by agencies and organisations, that the individual concerned would reasonably expect the agency or organisation to use the information for the secondary purpose in question. The ALRC agrees with the argument of the OPC and others that such a condition is a small but important protection against the misuse of an individual's personal information. The ALRC believes that such a requirement provides an added protection for individuals to require agencies, as well as organisations, only to use and disclose personal information for appropriate purposes.

22.44 This condition is not particularly onerous, given that it is an objective test that does not require an agency or organisation to consult the individual on each proposed secondary use or disclosure of the individual's personal information. It is unlikely to hamper an agency or organisation in providing a service to an individual because it is strongly arguable, as the OPC submitted, that such a requirement is already implied in IPP 10.1(e). If a primary purpose is related to a secondary purpose, it is likely that an individual would reasonably expect the data collector to use or disclose his or her personal information for that secondary purpose. In this way, one of the main effects of the additional reasonable expectation requirement is to remove any potential ambiguity as to the scope of the secondary use and disclosure exception.

---

45 The issue of 'bundled consent' is discussed in Ch 16. See, especially, Proposal 16–1.

46 See Part H.

Proposal 22–2 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the:

(a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.

Emergencies, disasters and threats to life or health

Background

22.45 Particular issues are raised when it is necessary to handle personal information after, or during, an emergency, disaster or some other kind of threat to a person's life or health. Under the *Privacy Act*, there are currently four alternative regimes for handling personal information in such situations:

- under the IPPs, if the personal information is to be handled by an agency;
- under the NPPs or an approved privacy code, if the personal information is to be handled by an organisation;
- subject to the rules on collection, use and disclosure in Part VIA of the Act, if there is the requisite connection to an emergency that has been the subject of a ministerial declaration;[47] or
- without reference to any of the above rules, if the act or practice is the subject of a temporary public interest determination made by the Privacy Commissioner in conformity with Division 2 of Part VI of the Act.[48]

22.46 This part of the chapter considers the handling of personal information under the privacy principles. As noted above, Part VIA provides a separate regime for the handling of personal information in the event of a declared emergency. Part VIA was recently introduced into the Act, commencing operation on 7 December 2006—after

47 The Part VIA regime is discussed in Ch 40.
48 Temporary public interest determinations are discussed in Ch 44.

the release of IP 31.[49] It does not alter the IPPs or NPPs themselves; rather, it displaces some of the requirements in the IPPs and NPPs by providing a separate regime for the collection, use and disclosure of personal information where there is the requisite connection to an emergency that has been the subject of a declaration by the Prime Minister or a Minister. Given that some of the problems with the IPPs and NPPs in this area may have been obviated by the introduction of Part VIA, this part of the chapter considers the following question: what reforms are needed to the privacy principles to deal with personal information handling in emergency situations that are not subject to the Part VIA regime?

22.47 Both the IPPs and NPPs provide for personal information to be used and disclosed, subject to conditions, in certain emergency situations. For agencies, IPPs 10 and 11 permit a record-keeper to use or disclose personal information for a secondary purpose provided he or she reasonably believes this is necessary to prevent or lessen a serious and imminent threat to a person's life or health.[50]

22.48 NPP 2 contains two similar exceptions that permit an organisation to use or disclose personal information for a secondary purpose where:

- the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety; or

- in the case of an individual's genetic information, the organisation reasonably believes the use or disclosure to a genetic relative of the individual is necessary to lessen or prevent a serious (but not necessarily imminent) threat to the life, health or safety of a genetic relative of the individual.[51]

22.49 Stakeholders identified several practical problems arising from the operation of these provisions. These concerns led the ALRC to ask in IP 31 whether agencies and organisations should be permitted to use or disclose personal information 'where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to an individual's safety or welfare, or a serious threat to public health, public safety or public welfare'. The ALRC also asked how the use and disclosure principle should deal with 'times of emergency'.[52]

Submissions and consultations

22.50 Both the IPPs and NPPs permit disclosure in the event of certain 'serious and imminent' threats. In relation to the IPPs, the Community Services Ministers' Advisory Council expressed concern that the desire by agencies to protect individuals' privacy

---

49 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).
50 *Privacy Act 1988* (Cth) s 14, IPP 10.1(b), 11.1(c).
51 The operation of this exception is considered in Part H.
52 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–7.

can make them unwilling to disclose personal information, and this can, at times, hamper the protection and care of vulnerable people. The Council argued it was too difficult to establish that a threat to a person's life or health was both 'serious and imminent' in order to justify a disclosure, stating:

> Other legislation, such as in the child welfare arena, enables the sharing of information when there is 'reasonable suspicion' or concern of abuse and risk. This is a lower threshold, often more appropriate in the case of vulnerable people, and more fitting with the concepts of early intervention and practice.[53]

22.51 In relation to the NPPs, concern was expressed, before Part VIA of the Act was introduced, that NPP 2 does not cater adequately for the disclosure of personal information by organisations to government agencies and other relevant bodies to deal with emergencies and disaster recoveries where the relevant threat is not both 'serious' *and* 'imminent'. For example, after an offshore natural disaster has occurred, a threat to a person's safety may no longer be 'imminent'. However, for identification purposes and to provide information to family members, the Australian Government Department of Foreign Affairs and Trade (DFAT) may need to ascertain—for example, from an airline or travel agent—whether a particular individual was in the affected location at the time of the disaster.[54] If the situation in question is covered by Part VIA of the Act, this problem no longer exists. A question remains, however, as to whether the privacy principles should also be amended to make it easier to share personal information in an emergency situation that is not covered by Part VIA.

22.52 A large number of stakeholders submitted that there should be a dilution of the requirement that a threat be *both* imminent *and* serious before personal information can be used or disclosed under the IPPs and NPPs. Reasons for this include that the current provision:

- operates as a barrier to stop agencies from doing what is necessary to meet 'a credible threat';[55]
- discourages officers from the Australian Government Department of Immigration and Citizenship from sharing information with officers of the Family Court of Australia in respect of a child under the Court's jurisdiction who may be likely to be abducted;[56]

---

53 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

54 Australian Government Department of Foreign Affairs and Trade, *Consultation PC 10*, Canberra, 29 March 2006.

55 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

56 Confidential, *Submission PR 214,* 27 February 2007.

- encourages differing interpretations and 'erring on the side of caution, or non-disclosure, in order to protect perceived agency or professional interests (which does not necessarily support the safety of the individuals concerned)';[57] and

- creates a 'catch 22' situation because sometimes a proper assessment of whether a threat is serious and imminent can only be made after the relevant person is aware of the personal information in question.[58]

22.53 Some stakeholders suggested alternative formulations of the threat level requirement. Two stakeholders submitted that the threat level should be 'serious *or* imminent', as distinct from 'serious *and* imminent'.[59]

22.54 A number of stakeholders submitted that the test should simply be whether the threat is 'serious'—that is, the requirement that the threat also be 'imminent' should be removed.[60] The NHMRC stated that 'the requirement for a threat to be imminent creates additional interpretive uncertainty'.[61] The Government of South Australia submitted that the requirement of imminence 'may fuel escalation of a crisis' and 'can also be difficult to establish because the information about the extent and nature of a threat is held by another party'.[62] It was also noted that removing the 'imminent' element of the exception would enhance consistency across legislation dealing with privacy, secrecy and confidentiality.[63]

22.55 Some stakeholders preferred a different formulation altogether, with some suggesting that the exception should apply where the threat level is 'significant', the definition of which may involve a balancing process between the public interest and privacy implications of disclosure.[64]

22.56 Other stakeholders proposed greater specificity in the wording of the exception, enabling disclosure where the person reasonably believes it is necessary to protect a child from abuse or neglect.[65]

---

57 Government of South Australia, *Submission PR 187,* 12 February 2007.
58 Ibid.
59 Australian Federal Police, *Submission PR 186,* 9 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
60 Government of South Australia, *Submission PR 187,* 12 February 2007; Confidential, *Submission PR 143,* 24 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
61 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
62 Government of South Australia, *Submission PR 187,* 12 February 2007.
63 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
64 Confidential, *Submission PR 130,* 17 January 2007. See also Government of South Australia, *Submission PR 187,* 12 February 2007.
65 Confidential, *Submission PR 214,* 27 February 2007. A similar point is made in Government of South Australia, *Submission PR 187,* 12 February 2007.

22.57 The OPC favoured the retention of the condition that a relevant threat be both serious and imminent. It submitted that:

> Should the gravity of the threat not involve a measure of imminence, then the individual should retain the usual level of privacy protection as other mechanisms may be available to provide for the disclosure of the information. For example, an agency or organisation could seek the individual's consent before disclosure of personal information occurs (should none of the other exceptions apply).[66]

22.58 The OPC further argued that the advent of Part VIA and the public interest determination provisions adequately address the concerns of DFAT and others about sharing information in emergency situations.[67]

ALRC's view

22.59 The ALRC shares the view of a large number of stakeholders that the current exceptions in respect of emergency situations are too narrow. The main problem seems to relate to the exception where the data collector reasonably believes that secondary use or disclosure 'is necessary to lessen or prevent … a serious and imminent threat to an individual's life, health or safety'.[68] There is considerable concern that the requirement that the threat must be both serious *and* imminent is too difficult to satisfy and that it can lead to personal information not being used or disclosed in circumstances where it should be. The ALRC agrees that this test is too difficult to satisfy and that it should be relaxed.

22.60 Three main alternative terms were suggested by stakeholders. The first suggestion was that the conjunctive *and* in the term 'serious and imminent' should be replaced by the disjunctive *or*. This would allow secondary use or disclosure where the relevant threat is either serious or imminent. The ALRC believes, however, that where a threat is merely imminent, but not serious, this is not enough to displace the presumptive position that an individual's personal information will not be used or disclosed for a secondary purpose.

22.61 The ALRC believes that any analysis of whether a threat is 'serious' must involve consideration of the gravity of the potential outcome as well as the relative likelihood. Take, as a hypothetical example, the threat to an individual sitting under a tree that he or she will be struck by a falling tree branch. One could sensibly argue that the threat is imminent in that a breach could fall at any time. Assessing whether the threat is serious with reference to the potential outcome may lead one to the conclusion

---

66 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

67 Ibid.

68 See *Privacy Act 1988* (Cth) sch 3, NPP 2.1(e)(i). Note that the use and disclosure principles in the IPPs contain provisions that are substantively similar. The difference is that they relate only to threats to an individual's 'life or health' without mentioning the additional category of 'safety': see IPPs 10.1(b) and 11.1(c).

that the threat is indeed serious because, if a heavy branch landed on the individual's head, it could injure or kill him or her. To end the analysis here, however, would be premature because, in the ordinary course of events, it is very unlikely that a branch would fall on the individual at precisely the time he or she is sitting under the tree. In other words, if a threat carries a potentially grave outcome but is highly unlikely to occur, it is not 'serious', in the sense that it should not cause us to alter one's course of conduct in any meaningful way.

22.62 In summary, therefore, the ALRC's view is that there should not be an exception to the general prohibition against secondary purpose use or disclosure to cover threats that the vast majority of people consider to be tolerable. It would be a significant dilution of an individual's privacy rights if the exception were to apply to imminent, but non-serious, threats.

22.63 Some stakeholders suggested replacing the term 'serious and imminent' with 'significant'. The problem with this suggestion is that the term 'significant' does not have a particular meaning in this context and would need to be explained further. Such an amendment could cause further ambiguity.

22.64 The third, and most popular, suggestion was to delete the words 'and imminent', thereby making the exception applicable where the relevant threat is serious, but not necessarily imminent. The ALRC prefers this approach because it would allow an agency or organisation to take preventative action to stop a threat from developing to a point where the danger, which one is seeking to avoid, is likely to eventuate. As a number of stakeholders have observed, at this point it is often too late to take meaningful preventative action. Unlike the first option noted above, the ALRC believes that this formulation strikes an appropriate balance between respecting the privacy rights of an individual and the public interest in averting threats to people's life, health and safety.

22.65 Finally, the ALRC notes that the threat categories in NPP 2.1(e)(i) of 'life, health or safety' were not the subject of detailed comment by stakeholders. Neither were the threat categories in NPP 2.1(e)(ii)—namely, 'public health or public safety'—which currently operate only in relation to 'a serious threat'. The ALRC's view is that these categories remain appropriate.

Proposal 22–3 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.

Missing persons

Background

22.66 Concern has been expressed that the IPPs and NPPs do not cover adequately the disclosure of personal information to law enforcement authorities, and the use of the information by them, when undertaking functions that may not involve a criminal offence or breach of the law but are nevertheless in the public interest.[69] The archetypal example of this is missing person investigations by the police and others. The AFP observed that currently the Act 'arguably … denies a missing person the knowledge or right to know that their relatives and friends are looking for them'.[70]

22.67 IPP 11 has been seen as particularly problematic because it does not contain a note equivalent to that under NPP 2.1, which states that the principle is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions. In contrast, Tasmanian privacy legislation expressly allows the use and disclosure of personal information where the secondary purpose is the investigation of missing persons by a law enforcement agency.[71]

22.68 The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) identified problems in applying the NPPs in this area.[72] For example, the AFP noted the reluctance of some organisations to provide personal information due to: ignorance of the fact that the NPPs permitted them to do so for law enforcement purposes; concerns about disclosures being detrimental to commercial interests; the costs of complying with a request for information; and concerns about litigation by those to whom the information relates. The OPC stated that it would work with the law enforcement community, private sector bodies and community representatives to develop practical guidance to assist private sector organisations in understanding their obligations under the *Privacy Act*.[73]

22.69 In its submission to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry), the AFP noted that, while education may have a role to play in raising awareness, it was unlikely to offer a complete solution. It submitted that a possible solution might be to give it the power to issue a notice to produce.[74] The Senate Committee privacy inquiry supported the OPC's recommendation to develop practical guidance in this area, but considered that

---

69 See Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

70 Australian Federal Police, *Submission PR 186,* 9 February 2007.

71 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(1)(g)(vi).

72 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 223.

73 Ibid, rec 65.

74 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.119], [5.121].

the Australian Government should also consider additional mechanisms to resolve the issue.[75]

22.70 The ALRC asked in IP 31 whether the privacy principles should be amended expressly to allow agencies and organisations to use or disclose personal information to assist in the investigation of missing persons.[76]

Submissions and consultations

22.71 A number of stakeholders made the general submission that the *Privacy Act* should be amended so as better to assist the police in locating missing persons.[77] CrimTrac submitted that it is sometimes necessary for police to share information such as criminal records to assist in searching for missing persons.[78]

22.72 The AFP suggested the solution to this problem could involve the following steps: (a) permitting disclosure under the IPPs in respect of 'serious *or* imminent' threats; (b) re-wording IPPs 10 and 11 'using NPP 2.1(h) as the starting point'; and (c) codifying Public Interest Determinations 3A, 4 and 5.[79] These permit the AFP to disclose, respectively: serious misconduct; certain information in relation to insurance claims or civil litigation; and certain information for research purposes.

22.73 Major Kathy Smith of the Salvation Army Family Tracing Service (South Australia) submitted that the *Privacy Act* should be amended to allow the Service to be 'given information or confirmation of the whereabouts of the person we are looking for', given its role in reuniting family members who have become separated.[80] In relation to organisations being able to access personal information for the purposes of locating missing persons, the Office of the Information Commissioner Northern Territory stated:

> There is justification for allowing organisations and agencies to assist law enforcement bodies in searches for missing persons. However, I would have some concern with a blanket unconditional approval for assistance to private sector organisations.[81]

22.74 The Institute of Mercantile Agents suggested a more extensive amendment to permit all private and public sector entities that deal with missing persons to 'have regulated and audited access to locator information'. In particular, it believes that its members should have access to such locator information because 'the costs of missing

---

75 Ibid, [7.52].
76 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–7(a).
77 CrimTrac, *Submission PR 158,* 31 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
78 CrimTrac, *Submission PR 158,* 31 January 2007.
79 Australian Federal Police, *Submission PR 186,* 9 February 2007.
80 K Smith, *Submission PR 246,* 8 March 2007. See also Salvation Army, *Submission PR 15,* 2 June 2006.
81 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

persons not meeting their obligations' amounts to at least four billion dollars annually.[82]

22.75 On the other hand, some stakeholders resisted any change to the privacy principles in respect of missing persons, noting that sometimes a missing person has committed no offence and does not wish to be located.[83] The OPC stated that the power to issue public interest determinations adequately covers the situation of missing persons.[84]

ALRC's view

22.76 The ALRC's view is that a number of amendments proposed elsewhere in this Discussion Paper would assist in alleviating the problems in relation to missing persons. First, in the context of missing persons, the threat to an individual will often be serious but it may be difficult to prove that it is also imminent. Proposal 22–3 would allow for the secondary use or disclosure of personal information where it is necessary to lessen or prevent a serious threat to an individual's life, health or safety. This means that an agency or organisation would no longer be required to show that the threat is both serious *and* imminent.

22.77 Secondly, as set out in the proposed UPPs, the ALRC believes that the exception in current NPP 2.1(h) should apply also to agencies.[85] This provides a broader scope to use or disclose personal information for a secondary purpose in the law enforcement area than is currently provided under the IPPs. Both of these proposed amendments respond to suggestions made by the AFP, which is one of the most important bodies involved in searching for missing persons.

22.78 The ALRC does not believe, however, that it is desirable to create further specific exceptions in respect of missing persons. As a number of stakeholders pointed out, sometimes a missing person has committed no offence and does not wish to be located. There are also situations where a person, deemed missing, may be seeking to hide themselves, not from the lawful authorities, but from other individuals who wish to do them harm. An example of such a situation is where a person is fleeing domestic violence. To provide a more general exception in respect of missing persons would risk endangering the privacy and other rights of these people.

---

82 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

83 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

84 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. The Privacy Commissioner can make a temporary public interest determination where an urgent decision needs to be made that the Commissioner believes may be breach the IPPs or NPPs. Such a determination effectively gives immunity to the agency or organisation subject to the determination in respect of the breach. See *Privacy Act 1988* (Cth) pt VI, div 2. Public interest determinations are discussed in detail in Ch 44.

85 See the UPPs, which are set out at the beginning of this Discussion Paper.

22.79 Finally, where an agency or organisation has a legitimate reason to search for a missing person, it may often be able to avail itself of one of the other exceptions in the use and disclosure principle, or it may seek a public interest determination.[86]

Disclosure of 'incidents' by insured professionals to insurers

22.80 In IP 31, the ALRC asked whether the exceptions in NPP 2 are adequate to cover: (a) disclosures by a professional of a client's personal information pursuant to an indemnity insurance contract where the provision of professional services has led to an adverse outcome; and (b) on-disclosures by insurers to members of their 'cases committees', often comprising experts in the relevant profession, who advise insurers about making provision for possible future claims.[87]

22.81 For example, a doctor may need to disclose the existence of an incident to his or her insurer so that the insurer can assess the legal risk and make financial provision for a possible future claim. The incident may or may not mature into a legal claim. While disclosure of the doctor's personal information to the insurer occurs with consent, the legality of the disclosure of the patient's personal information is less clear.

22.82 If an organisation seeks to rely on NPP 2.1(a) and the disclosure involves sensitive information, such as health information, this requires that the purpose of advising in relation to indemnity be 'directly related' to the primary purpose of collection of the patient's information—that being the care and treatment of the patient. It is unlikely that a 'direct' relation could be made out. In addition, NPP 2.1(a) requires that the individual would reasonably expect the doctor to disclose his or her personal information to the doctor's insurer following an incident. Many patients may not have considered this. Such disclosure would, however, be lawful if: (a) the patient were required to consent to possible disclosures to insurers and their case committees as a condition to obtaining the health service;[88] or (b) if the common law or legislation authorised the disclosure of a client's personal information to an insurer prior to any claim being made.

22.83 The ALRC asked whether there should be an express secondary use exception in NPP 2 to allow for disclosures of incidents to insurers, or whether the issue should be dealt with by way of a public interest determination.[89]

Submissions and consultations

22.84 UNITED Medical Protection submitted that NPP 2.1(g) already provides for disclosure of incidents by professionals to their professional indemnity insurers.[90]

---

86 Public interest determinations are discussed in Ch 44.
87 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.84].
88 'Bundled' consent is discussed in detail in Ch 16.
89 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.84]–[4.86].
90 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

NPP 2.1(g) permits secondary use or disclosure where it is 'required or authorised by law'. Its relevance here is that a prospective insured is legally required to inform an insurer of facts and circumstances that might give rise to a claim when applying for insurance.[91] UNITED Medical Protection noted that this can also be

> a contractual necessity, which is in the interests of both the professional and patient in the event of a claim being made against the professional. The last thing a patient would want in the event of a claim is for the professional to be un-insured for the claim.[92]

22.85 UNITED Medical Protection submitted that disclosure in these circumstances would satisfy both limbs of current NPP 2.1(a). First, notifying a professional indemnity insurer or lawyer of an adverse incident or threatened litigation is a directly related secondary purpose. Secondly, it was submitted that 'patients these days are aware of their entitlement to commence legal proceedings for damages in the case of perceived medical negligence and that the doctor will be covered by his or her professional indemnity insurance'.[93]

22.86 Nevertheless, some stakeholders submitted that further clarification is warranted. UNITED Medical Protection submitted that the situation where professionals make disclosures to their professional indemnity insurer should be dealt with either by way of an exception in the use and disclosure principle or by adopting a public interest determination.[94] Similarly, the Australian Bankers' Association suggested that the best solution would be to provide an express secondary use and disclosure exemption 'to allow for disclosure of incidents to insurers' and to facilitate the provision of information to alternative dispute resolution schemes.[95]

ALRC's view

22.87 The ALRC's view is that the existing exceptions to the secondary use and disclosure prohibition are sufficient to cover this situation and no new exception needs to be added. Both of the exceptions noted above are reproduced, in like form, in the 'Use and Disclosure' principle in the proposed UPPs.

22.88 In relation to the exception where the secondary use or disclosure is required or authorised by law, the ALRC agrees that s 21 of the *Insurance Contracts Act 1984* (Cth) would permit disclosure to insurers in a number of relevant circumstances. To the extent that this provision does not cover the full spectrum of disclosures that can

---

91 See *Insurance Contracts Act 1984* (Cth) s 21.
92 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.
93 Ibid.
94 Ibid.
95 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

legitimately be made to insurers, however, the ALRC believes that the related use or disclosure exception—currently set out in NPP 2.1(a)—is sufficient.

22.89 On the related use exception, the ALRC believes that the requirement can be satisfied in these circumstances. In the health context, the OPC has already issued guidance that states, relevantly:

> Directly related secondary purposes may include many activities or processes necessary to the functioning of the health sector.
>
> Where the use or disclosure of de-identified data will not suffice, and provided it is within the reasonable expectations of the individual, no extra steps need be taken when using or disclosing relevant personal information in circumstances, such as: …
>
> - billing or debt-recovery;
> - an organisation's management, funding, service-monitoring, complaint-handling, planning, evaluation and accreditation activities—for example, activities to assess the cost effectiveness of a particular treatment or service;
> - disclosure to a medical expert (only for medico-legal opinion), insurer, medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example in reporting an adverse incident;
> - disclosure to a lawyer for the defence of anticipated or existing legal proceedings; [and]
> - an organisation's quality assurance or clinical audit activities, where they evaluate and seek to improve the delivery of a particular treatment or service … .[96]

22.90 This makes clear that disclosures of incidents to insurers, in all appropriate circumstances, are covered in the 'directly related' limb of the exception. Furthermore, the ALRC agrees with the submission of UNITED Medical Protection that it would fall within the reasonable expectation of an individual for secondary disclosure to occur in these circumstances.

22.91 In light of the above, the ALRC is of the view that it is unnecessary to include an additional exception in the use and disclosure principle to allow for disclosures of incidents to insurers. Nor is it presently necessary to deal with this issue by way of a public interest determination.

Use and disclosure in other contexts

Where required or authorised by or under law

22.92 Currently, NPP 2.1(g) and IPPs 10.1(c) and 11.1(d) permit use or disclosure for a secondary purpose where this is 'required or authorised by or under law'. Consistently with the discussion in Chapter 13, the ALRC is interested in the views of

---

96 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).

stakeholders on the question whether this exception should be narrowed to allow secondary purpose use or disclosure where this 'is required or *specifically* authorised by or under law'. Such a provision would require legislative consideration of whether the particular type of secondary use or disclosure in question ought to be permitted before an agency or organisation would be able to take advantage of this exception.

22.93 Arguably, such an amendment might bring the relevant exception more in line with its intended operation. The relevant Explanatory Memorandum accompanying the introduction of NPP 2.1(g) states:

> The sub-principle is intended to cover situations where a law unambiguously requires or authorises the use or disclosure of personal information. There could be situations where the law requires some actions which, of necessity, involve particular uses or disclosures, but this sort of implied requirement would be conservatively interpreted. The reference to 'authorised' encompasses circumstances where the law permits, but does not require, use or disclosure.[97]

22.94 The OPC, for example, suggested that this exception should be narrowed with respect to the use or disclosure of sensitive information. It submitted that 'to avoid a broad reading of this [exception] where sensitive information is at stake, the inclusion of "clearly" or "expressly" authorised could be considered'.[98]

22.95 The ALRC is aware that such an amendment could possibly have unintended consequences in certain areas. For example, such an amendment may serve as an impediment on agencies that are presently relying on the current, broadly worded exception to carry out their statutory functions, such as to monitor service delivery. Therefore, the ALRC is soliciting views on whether such an amendment is appropriate and desirable.

Question 22–1 Should the proposed 'Use and Disclosure' principle contain an exception allowing an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of collection where this is 'required or *specifically* authorised by or under law' instead of simply 'required or authorised by or under law'?

Due diligence

22.96 An issue raised in the OPC Review was whether the practice of due diligence on the sale and purchase of a business raises any particular concerns in the application of

97 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [336].
98 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

the privacy principles.[99] The issue of due diligence in the context of mergers and acquisitions has also been raised in this Inquiry.[100] A prospective purchaser of a business undertakes a process of due diligence to assess the value of the business' assets and liabilities. This process may involve the collection and disclosure of personal information about employees, customers, trading partners and business associates.

22.97 In 2002, the OPC issued an information sheet in relation to the obligations of buyers and sellers under the *Privacy Act*.[101] The OPC reported that it had not received a complaint about a breach of privacy during a due diligence exercise. It stated that it is not practical to require an organisation in the process of due diligence to gain the consent of everyone whose personal information is transferred and it recommended that the Australian Government should consider amending the NPPs to take into account the practice of due diligence.[102] New Zealand law, for instance, allows disclosure of information where 'it is necessary to facilitate the sale or other disposition of a business as a going concern'.[103]

22.98 The ALRC solicited views as to whether such amendment is necessary, and if so, what form it might take. It is also asked for views about whether there is a need to amend Information Sheet 16 in this regard.[104] Only the Queensland Council for Civil Liberties made a submission on this issue. It argued that if 'a flexible and pragmatic approach' is taken to the application of the privacy principles, no privacy issues would arise in relation to due diligence. However, it was open to the possibility of amending the Act if there is a 'serious concern' about this.[105]

ALRC's view

22.99 The ALRC believes that the use and disclosure principle clearly was not intended to impede genuine due diligence, provided it is carried out lawfully. Consequently, the ALRC shares the view of the Queensland Council for Civil Liberties that, provided the use and disclosure principle is interpreted purposively, there is no need to create a new exception dealing with the use and disclosure of personal information in the course of due diligence.

22.100 The fact that few stakeholders have identified a problem in this area seems to indicate that the privacy principles are being applied appropriately. Moreover, the

---

99 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), [6.11].

100 G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.

101 Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002).

102 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 191 and rec 57.

103 *Privacy Act 1993* (NZ) s 6, Principle 11.

104 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.106]–[4.107].

105 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

ALRC is of the view that the guidance already provided by the OPC, especially in Information Sheet 16, is sufficient.

Research, health care and disclosure on compassionate grounds

22.101 A number of the exceptions in the current use and disclosure principle in NPP 2 deal with research and health care. These will be dealt with in Part H of this Discussion Paper, with a view to moving these provisions out of the 'Use and Disclosure' principle in the proposed UPPs and into more specific subordinate legislation.

22.102 Specifically, the following exceptions to NPP 2 will be considered as follows:

- The exception in NPP 2.1(d) dealing with health information to be used or disclosed for the secondary purpose of research, or the compilation or analysis of statistics, relevant to public health or public safety will be dealt with in Part H.

- The exception in NPP 2.1(ea) dealing with genetic information obtained in the course of providing a health service will be dealt with in Part H.

- The provisions in NPP 2.4–2.6 dealing with the disclosure of health information by a health service will be dealt with in Parts H and I.

22.103 There is also an issue about individuals being able to obtain information about family members and friends in an emergency, where this does not fall within the Part VIA regime. The OPC Review suggested that NPP 2 could be amended to deal with emergencies by allowing for disclosure based on compassionate grounds to a person 'responsible' for the individual where the individual is unable to consent to the disclosure and it is not contrary to any wish expressed by the individual.[106]

22.104 Under NPP 2.5, a person 'responsible' for the individual includes various specified family members as well as a person nominated by the individual to be contacted in times of emergency. The OPC recommended that the definition should be extended to include a person nominated by the family to act on its behalf.[107] A number of stakeholders agreed with this suggestion.[108] This issue is dealt with in Part H.

---

106 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 236; rec 68.

107 See Ibid, rec 68.

108 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; AAMI, *Submission PR 147,* 29 January 2007.

Logging disclosures

Background

22.105 In Question 4–10 of IP 31, the ALRC asked whether agencies or organisations should be required to record their use or disclosure of personal information when this occurs for a purpose other than the primary purpose of collection. This invited reconsideration of one of the issues previously considered by the ALRC in its 1983 report, *Privacy* (ALRC 22). In that report, the ALRC did not recommend that record-keepers be obliged to keep a log of all uses and disclosures of personal information because the administrative costs would be too high. Instead, it suggested that the Human Rights Commission (as it was then called) should encourage record-keepers to adopt the practice of logging disclosures, at least those disclosures that would represent an especially objectionable interference with individual privacy.[109]

22.106 Under NPP 2, an organisation is only required to make a written note of its use or disclosure of personal information where it relates to a specified law enforcement purpose.[110] NPP 2 has been criticised on the basis that it does not require organisations to record their use and disclosure of personal information in times of emergencies 'to ensure that a trace of the activities of privacy-abusers is retained'.[111]

22.107 Similarly, IPPs 10 and 11 require an agency to make a written note of its use and disclosure of information only where it is for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue. In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that every agency should keep a record of authorised disclosures of confidential third party information for the purpose of checking the legitimacy of access to such information. It recommended that the record should include the names of individuals and organisations about whom information is disclosed, the names of the individuals and organisations to whom that disclosure is made, and the date of the disclosure.[112]

Submissions and consultations

22.108 A number of stakeholders suggested that agencies and organisations should be required to record when they have used or disclosed personal information for a secondary purpose. Some suggested that this requirement should apply to all secondary

---

109 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Vol 2, 197.

110 See *Privacy Act 1988* (Cth) sch 3, NPP 2.2.

111 R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 177.

112 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), rec 6.

purpose use or disclosure.[113] Others stated that the requirement should only apply where there is not a direct link between the primary and secondary purpose.[114] The Queensland Government submitted that a more general requirement may result in an 'undue administrative burden'.[115]

22.109 The NHMRC agreed that such recording represented good practice, but submitted that a 'requirement will impose significant burdens and costs'. It advocated 'an educative approach that highlights the various ways in which information transactions can be recorded and the benefits of doing so where practicable'.[116]

22.110 Some stakeholders were opposed to any such recording requirement. It was submitted that the existing requirements are 'an unmanageable burden' and that any extension would be 'potentially onerous',[117] and would increase the cost of compliance.[118] UNITED Medical Protection stated that such a requirement would place particular burden on medical practices because considerable time and cost would be required to create the logging system and then to carry out the logging process.[119]

22.111 This assertion was queried, however, with respect to electronic data,[120] and it was noted that such a requirement already applies to South Australian government agencies under the Adequate Records Management Standard.[121] It was suggested that if the requirement 'were limited to a high, policy level' addressing information handling practices, this would reduce the regulatory burden.[122]

22.112 The AFP argued that a recording requirement would not 'enhance the current accountability framework' and may lead to duplication.[123] Similarly, UNITED Medical Protection argued that a better way to protect privacy is through appropriate limitations on use and disclosure.[124]

---

113 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; I Turnbull, *Submission PR 82,* 12 January 2007. In fact, one stakeholder stated that the obligation should apply to primary and secondary use or disclosure: Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

114 Queensland Government, *Submission PR 242,* 15 March 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; AAMI, *Submission PR 147,* 29 January 2007.

115 Queensland Government, *Submission PR 242,* 15 March 2007.

116 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

117 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

118 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

119 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

120 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

121 Government of South Australia, *Submission PR 187,* 12 February 2007.

122 Ibid.

123 Australian Federal Police, *Submission PR 186,* 9 February 2007. See also Law Council of Australia, *Submission PR 177,* 8 February 2007.

124 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

22.113 In terms of how a recording obligation might operate in practice, the following suggestions were made:

- the requirement should be for any form of record that allows: reconstruction in the event of an inquiry or challenge; notification of third parties where information is later corrected; and notification of individuals following a security breach;[125]

- individuals should be able to access the logs that relate to themselves;[126]

- there should be no recording requirement where the individual has consented to the use or disclosure,[127] or where he or she is already aware of the use or disclosure;[128] and

- the recording requirement should be framed so as not to impact adversely on the privacy of third parties—for example, by collecting the personal information of a third party.[129]

ALRC's view

22.114 The ALRC does not believe that it is desirable to require agencies and organisations to record their use or disclosure of personal information when this occurs for a purpose other than the primary purpose of collection. While such a requirement may be a benefit to individuals in helping them, for example, to trace how their personal information is used and disclosed after it has been collected, the ALRC's view is that, on balance, the disadvantages of such a requirement would outweigh the benefits.

22.115 First, as was pointed out by a number of stakeholders, such a requirement will in many cases be very onerous for agencies and organisations, and particularly for those that handle large amounts of personal information. It would also be of limited benefit to individuals. To the extent that such a provision is likely to be useful to individuals, it would duplicate requirements in the privacy principles dealing with data quality and data security.[130]

22.116 Secondly, the ALRC's proposal to insert provisions that oblige agencies and organisations to provide notification where personal information has been compromised—a phenomenon referred to commonly as a 'data breach'—is likely to deal more effectively with errors in the handling of personal information. As explained

---

125 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
126 Law Council of Australia, *Submission PR 177,* 8 February 2007.
127 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; AXA, *Submission PR 119,* 15 January 2007.
128 AXA, *Submission PR 119,* 15 January 2007.
129 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
130 See Chs 24 and 25 respectively.

in detail in Chapter 47, the ALRC proposes that agencies and organisations should be required to report to the OPC and the individual concerned any data breach that results in a real risk of serious harm to the individual. This provision would be of greater utility than a general requirement to log all uses and disclosures of personal information because it focuses attention only on where some error has occurred in the handling of personal information.

22.117 Thirdly, as noted above, such a requirement already exists when an agency or organisation uses or discloses personal information under the relevant law enforcement exception.[131] The ALRC proposes that an equivalent provision be preserved in the proposed UPPs, and believes that this adequately addresses this issue.

Summary of proposed 'Use and Disclosure' principle

22.118 In summary, the ALRC's view is that the fifth principle in the proposed UPPs should be called 'Use and Disclosure'. It should appear as follows.

UPP 5. Use and Disclosure

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

(i) an individual's life, health or safety; or

131 See *Privacy Act 1988* (Cth) s 14, IPP 10.1(d), IPP 11.1(e); sch 3, NPP 2.1(h).

(ii) public health or public safety; or

(d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(e) the use or disclosure is required or authorised by or under law; or

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

5.2 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note: Agencies and organisations are also subject to the requirements of the 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

23. Direct Marketing

Contents

Introduction 699
Direct marketing generally 701
Submissions and consultations 701
ALRC's view 702
Scope of direct marketing privacy principle 703
Background 703
Submissions and consultations 703
ALRC's view 704
Relationship between privacy principles and other legislation 706
Background 706
Submissions and consultations 706
ALRC's view 707
Opt-in or opt-out requirement? 708
Background 708
Submissions and consultations 709
ALRC's view 710
Other possible requirements 713
Original source of personal information 713
Particularly vulnerable individuals 714
ALRC's view 714
Summary of proposed 'Direct Marketing' principle 716

Introduction

23.1 'Direct marketing' involves the promotion and sale of goods and services directly to consumers. Direct marketers compile lists of individuals' names and contact details from many sources, including publicly available sources such as the electoral roll, the telephone directory and land title registers. An individual may not always know that his or her personal information has been collected for the primary purpose of direct marketing.

23.2 The rules in the *Privacy Act 1988* (Cth) on direct marketing differ between organisations and agencies. The Information Privacy Principles (IPPs) do not contain any provisions dealing with direct marketing. In contrast, the National Privacy Principles (NPPs) limit the use and disclosure of personal information for the

secondary purpose of direct marketing. Under NPP 2.1(c), secondary purpose direct marketing is permitted only if all of the following conditions are met:

- the information in question is not 'sensitive information';
- it is impracticable to seek the individual's consent before using the information;
- the organisation will not charge the individual for giving effect to a request by the individual not to receive direct marketing communications;
- the individual has not requested the organisation to refrain from providing direct marketing communications;
- in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that the individual may express a wish not to receive any further direct marketing communications; and
- each written direct marketing communication to the individual sets out the organisation's business address and telephone number and, if the communication is made by electronic means, a number or address at which the organisation can be directly contacted electronically.

23.3 Issues arising from the practice of direct marketing and the application of the principles dealing with direct marketing were considered by the Office of the Privacy Commissioner's review of the private sector provisions of the *Privacy Act* (OPC Review).[1] These included whether:

- the *Privacy Act* should contain the assumption that personal information may be used for direct marketing;
- NPP 2.1(c) protects personal information adequately and, in particular, whether individuals should be given the opportunity to 'opt in' to direct marketing instead of having the choice to 'opt out'. If an 'opt-out' model is preferred, there was a question whether the Act should require organisations to comply with the 'opt-out' request within a specified time; and
- organisations should be required to advise individuals from where they acquired their personal information.

1 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 94–103.

23.4 This chapter covers the following main issues. First, it considers what should be the scope of the privacy principle dealing with direct marketing. Secondly, it considers how this principle in the *Privacy Act* should relate to other sectoral legislation that deals with particular types or aspects of direct marketing. Thirdly, it addresses the content of this principle and, in particular, whether an 'opt-in' or an 'opt-out' model should be accepted.

Direct marketing generally

23.5 Before the release of the ALRC's Issues Paper, *Review of Privacy* (IP 31), direct marketing was identified as a concern by a number of stakeholders. This was highlighted during the National Privacy Phone-In conducted by the ALRC on 1 and 2 June 2006 (the ALRC Phone-In), where 73% of calls identified as an issue of concern the receipt of unsolicited communication by way of phone, mail, fax, email and SMS. A number of the early submissions received by the ALRC also identified the practice of direct marketing as an area of concern.[2]

23.6 In IP 31, the ALRC asked the general question whether the privacy principles should permit non-sensitive personal information to be used for the secondary purpose of direct marketing and, if so, what should be the criteria for such use.[3]

Submissions and consultations

23.7 As well as those who expressed concerns about direct marketing generally,[4] a number of stakeholders observed that direct marketing serves some useful purposes and is important for the economy.[5] For example, the Australian Bankers' Association (ABA) submitted that it is essential for a long term, ongoing relationship between a business and its customer for the business to be able to stay in communication with its customer—and this is often facilitated by direct marketing.[6] Similarly, Australia Post submitted that if the Act were amended to

> inhibit the ability of a business to contact an unidentifiable party, there may be a significant decline in direct marking activities across Australia. This may give rise to

2 See, eg, S Alexander, *Submission PR 51,* 18 August 2006; L O'Connor, *Submission PR 35,* 2 June 2006; Confidential, *Submission PR 27,* 4 June 2006; Confidential, *Submission PR 13,* 26 May 2006.

3 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–12.

4 See, eg, Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; M Fenotti, *Submission PR 86,* 15 January 2007.

5 See, eg, Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Australia Post, *Submission PR 78,* 10 January 2007; The Mailing House, *Submission PR 64,* 1 December 2006.

6 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

> potentially serious economic consequences for both small and large businesses, and in particular, direct marketing organisations.[7]

23.8 It was also submitted that there are pragmatic reasons why those engaged in direct marketing do not wish to communicate with those who do not want to receive direct marketing communications. The Mailing House stated that the industry 'do[es] not wish to irritate the pubic, abuse the concept of privacy or incur expense on material that has little chance of influencing a response'.[8] Some stakeholders submitted that the existing direct marketing provisions were already too strict. For example, the Australian Health Insurance Association submitted:

> NPP 2.1 prevents health funds marketing other suitable products to members unless the individual's consent has been obtained 'before that particular use'. The requirements are impractical and inappropriate and should be changed to enable funds to engage in sensible direct marketing of their products in the best interests of their members. Reasonable information given by the fund and consent given by the member at the time of joining plus an opt-out provision, should be sufficient.[9]

ALRC's view

23.9 The issue of direct marketing has been, and continues to be, the subject of a very strong response from stakeholders and the community generally. On one hand, there is a strong push from consumers and consumer advocates to tighten the rules on direct marketing to make it more difficult for companies engaged in direct marketing to communicate with people in this way. This draws on the conceptualisation of privacy as including, at least, 'the right to be let alone'.[10]

23.10 On the other hand, business groups and others have emphasised the importance of direct marketing for the economy generally. They have also stressed that, if direct marketing is carried out appropriately, it can be of considerable assistance to consumers that receive direct marketing communications.

23.11 The ALRC's view is that it is possible to balance these competing positions by recognising both that some forms of direct marketing can be pernicious and can erode individuals' privacy rights but that, if undertaken appropriately, direct marketing also can be beneficial. The ALRC believes, therefore, that the optimum approach is to develop a regulatory regime that effectively balances these competing considerations.

---

7 Australia Post, *Submission PR 78,* 10 January 2007.

8 The Mailing House, *Submission PR 64,* 1 December 2006.

9 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

10 See S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 193. Note, however, that the definition of the 'right to privacy' should not be reduced only to the right to be left undisturbed. As explained in Chapter 1, the modern conceptualisation of privacy involves many other elements.

Scope of direct marketing privacy principle

Background

23.12 Before considering precisely how direct marketing should be regulated, it is necessary to consider the scope of the relevant privacy principle. This leads to two main questions. First, should this privacy principle apply without reference to whether the personal information in question was collected for the primary or secondary purpose of direct marketing?

23.13 As noted above, the *Privacy Act* currently deals with the issue of direct marketing as part of the use and disclosure principle in NPP 2. NPP 2 regulates how personal information may be used for a secondary purpose.[11] Therefore, given its location, the direct marketing requirements in NPP 2.1(c) operate only where the personal information in question was not collected for the *primary* purpose of direct marketing. The question, therefore, is whether the privacy principle should be extended to cover primary and secondary purpose direct marketing.

23.14 Secondly, assuming that the *Privacy Act* is amended to provide a single set of privacy principles applicable to the public and private sectors,[12] should the direct marketing privacy principle apply to agencies as well as organisations? This issue is of particular significance in light of the fact that the IPPs do not contain any provisions dealing with direct marketing by agencies.

Submissions and consultations

Extension to primary purpose direct marketing?

23.15 The Law Council of Australia submitted that there should be a separate privacy principle dealing with direct marketing, and that it should apply irrespective of whether the relevant personal information was collected for the primary purpose or a secondary purpose of direct marketing.[13] This is because the current provisions permit personal information that is collected for the primary purpose of direct marketing to be used 'almost without restraint'.[14] The Law Council submitted that:

> There appears to be no valid policy reason why an organisation which collects information for the primary purpose of direct marketing should be free to use that information in a way which organisations which collect it in the context of a relationship with the individual are not free to use it. Indeed, from a policy perspective you might expect fewer, not more, constraints on an organisation with which an individual has chosen to deal as opposed to an organisation which has no

11 The operation of NPP 2 is considered in greater detail in Ch 22.
12 See Proposal 15–2.
13 Law Council of Australia, *Submission PR 177,* 8 February 2007.
14 Ibid. See also Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.

> relationship with an individual but buys their information for the purpose of marketing to them.[15]

23.16 On the other hand, the Australian Direct Marketing Association (ADMA) submitted that an organisation should be required to make clear what is their primary purpose of collection and that, even where its primary purpose for contacting an individual is to engage in direct marketing, the organisation should provide an opportunity to opt out.[16]

Application of direct marketing principle to agencies?

23.17 In IP 31, the ALRC did not ask specifically whether agencies should be subject to a principle that restricts their ability to engage in direct marketing. Nevertheless, two submissions commented on this issue, arguing that the direct marketing provisions should be extended to cover agencies.[17] It was submitted that:

> Given that there are other means by which governments routinely communicate the availability of services (such as general advertising), it is difficult to see why government agencies should not have to respect a clearly expressed preference of individuals not to be contacted.[18]

23.18 Such a requirement could still be subject to certain exceptions, such as in respect of 'public health and safety campaigns'.[19]

ALRC's view

Extension to primary purpose direct marketing?

23.19 As noted above, the direct marketing provisions are currently dealt with as part of the use and disclosure principle in NPP 2. NPP 2 creates a general prohibition against the use or disclosure of personal information for a secondary purpose of collection, and then lists a number of exceptions to this general rule—one of which is for direct marketing, provided certain conditions are met.

23.20 The ALRC notes that there is currently considerable ambiguity as to whether organisations, which collect personal information that they later intend to use for direct marketing, have merely collected this information for the secondary purpose of direct marketing. There may also be some deliberate or unintended obfuscation. For example, where individuals are asked to provide personal information to make them eligible to win a prize, the individuals might assume that the primary purpose of the collection is to make them eligible for the prize, whereas the primary purpose of the organisation collecting this information may in fact be to create a database from which to carry out

---

15 Law Council of Australia, *Submission PR 177,* 8 February 2007.
16 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007.
17 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
18 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
19 Ibid; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

direct marketing.[20] This problem would be eliminated by making the direct marketing rules apply irrespective of whether the personal information in question was collected for the primary purpose of direct marketing or whether it was a secondary purpose.

23.21 The ALRC believes that the concerns expressed by stakeholders regarding the direct marketing activities of some organisations are unlikely to be addressed adequately if the relevant privacy principle only covers secondary purpose direct marketing. Consequently, the ALRC's view is that the Act should cover direct marketing undertaken by an organisation that has collected the individual's personal information for the primary purpose *or* a secondary purpose of direct marketing.

23.22 If this reform is adopted, the rationale for locating the direct marketing provisions in the general use and disclosure privacy principle is severely undermined. Moreover, given that direct marketing is relevant to other aspects of the information cycle—most notably, the collection of personal and sensitive information and the maintenance of data quality and data security—the ALRC believes that it is most logical to create a discrete privacy principle to regulate direct marketing.

Application of direct marketing principle to agencies?

23.23 If the direct marketing principle—in its current form or as proposed by the ALRC—is made applicable to agencies, this could have a significant impact on the way that government agencies communicate with individuals. Such a principle would have to be very carefully expressed so as not to preclude the legitimate communication of important information by agencies.

23.24 Given that IP 31 did not ask whether the direct marketing provisions in the privacy principles should apply to agencies, and given that few submissions have by addressed this issue, it would be premature for the ALRC to express a firm opinion on the desirability of such a reform. The ALRC remains interested in views on whether agencies should be subject to a privacy principle dealing with direct marketing and, if so, what should be the content of such a principle.

Proposal 23–1 The proposed Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' privacy principle. This principle should be called 'Direct Marketing' and it should apply irrespective of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing.

---

20 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 95.

Question 23–1 Should agencies be subject to the proposed 'Direct Marketing' principle? If so, should any exceptions or exemptions apply specifically to agencies?

Relationship between privacy principles and other legislation

Background

23.25 This part of the chapter considers how the privacy principle dealing with direct marketing should relate to sectoral legislation that deals with particular types or aspects of direct marketing. For example, some aspects of telemarketing are regulated by the *Do Not Call Register Act 2006* (Cth), and some aspects of email marketing are covered by the *Spam Act 2003* (Cth). This raises the question whether the regulation of direct marketing should be dealt with by a 'one size fits all' model in the privacy principles, or by sectoral legislation tailored to particular types of direct marketing, or a combination of both.

23.26 There are, in essence, three main options for reform. First, the proposed Unified Privacy Principles (UPPs) could refrain from dealing with direct marketing given that it is being regulated elsewhere. Secondly, the sectoral legislation that deals with specific types of direct marketing could be repealed, with the UPPs providing the sole form of regulation in respect of all forms of direct marketing. Thirdly, the UPPs could regulate direct marketing except to the extent that more specific sectoral legislation covers a particular aspect or type of direct marketing. The sectoral legislation could either provide more or less stringent privacy protection to this aspect or type of direct marketing.

Submissions and consultations

23.27 In the submission and consultation process, some stakeholders stated that it is unclear how the provisions in the NPPs dealing with direct marketing relate to the more specific sectoral legislation noted above, such as the *Do Not Call Register Act* and the *Spam Act*.[21] A number of suggestions were made to clarify the relationship between the direct marketing provisions in the privacy principles and similar provisions in other legislation.

23.28 The vast majority of stakeholders proceeded from the assumption that it is better to regulate direct marketing both by the privacy principles in the *Privacy Act* and sectoral legislation. It was submitted that the privacy principles should set minimum standards that apply generally, except where other more specific legislation applies.[22]

---

21 See, eg, AAMI, *Submission PR 147,* 29 January 2007.

22 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

23.29 A number of stakeholders submitted that such sectoral legislation should be 'consistent' with the *Privacy Act*.[23] Some refined this proposition to mean that the *Privacy Act* should contain minimum standards and, where sectoral legislation applies, that sectoral legislation should only impose stricter standards than those contained in the privacy principles on the use and disclosure of personal information for direct marketing.[24]

23.30 The Australian Privacy Foundation observed that such sectoral legislation would be unnecessary if the use and disclosure principle functioned properly and if there were adequate sanctions and active enforcement.[25] It was also submitted, however, that, given the broad exemptions provided for in the *Do Not Call Register Act* and the *Spam Act*, it will remain necessary for the *Privacy Act* also to cover direct marketing.[26]

ALRC's view

23.31 Consistently with the majority of stakeholders who commented on this issue, the ALRC's view is that the proposed 'Direct Marketing' principle should set out general requirements with respect to direct marketing, but these requirements should be able to be displaced by more specific legislation that deals with a particular type or aspect of direct marketing. This would allow, for example, the direct marketing principle in the *Privacy Act* to operate alongside the more specific provisions in the *Do Not Call Register Act* and the *Spam Act*.

23.32 The ALRC believes this approach is preferable to the other main options for regulating direct marketing. Imposing a blanket rule for all types and aspects of direct marketing is too rigid. For example, there is a strong view in the community that some forms of direct marketing are, or have the capacity to be, more intrusive than others. Clearly, those forms of direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing. Indeed, this explains the advent of sectoral legislation such as the *Do Not Call Register Act* and the *Spam Act*. Similarly, relying on such sectoral legislation to the exclusion of the *Privacy Act* is problematic, because it leaves loopholes that could encourage other types of direct marketing that may also be intrusive.

23.33 On the other hand, making clear that the direct marketing principle in the *Privacy Act* sets out the general requirements in this area, and that these general

---

23 ANZ, *Submission PR 173,* 6 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

24 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

25 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

26 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

requirements may be displaced by other requirements in certain contexts where Parliament deems it appropriate, allows for a regime that is more responsive to the specific needs of consumers and business.

23.34 Finally, the ALRC does not believe that the requirements of the proposed 'Direct Marketing' principle should only be able to be displaced by *more* onerous requirements in sectoral legislation. While such an approach may be superficially appealing to those opposed to direct marketing, it would limit Parliament's options when considering whether to pass sectoral legislation dealing with specific aspects of direct marketing. This, in turn, would ultimately undermine the responsiveness of the regime to the specific needs of a particular aspect or type of direct marketing.

Proposal 23–2 The proposed 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.

Opt-in or opt-out requirement?

Background

23.35 The Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry) recommended that the ALRC consider the possibility of an 'opt-in' regime for direct marketing in line with the *Spam Act*.[27] The OPC recommended that the Australian Government consider amending the *Privacy Act* to provide that consumers have a general right to opt out of direct marketing approaches at any time, and also to impose an obligation on organisations to comply with opt-out requests within a specified time after receipt.[28]

23.36 Some overseas privacy legislation, such as that in force in Hong Kong, provides for an 'opt-out' model.[29] A similar approach is taken in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data* (1995) (EU Directive).[30] A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under art 29 of the EU Directive, commented that 'where data are transferred for

27 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 15.

28 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 23.

29 See *Personal Data (Privacy) Ordinance* (Hong Kong) s 34.

30 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 14(b).

the purposes of direct marketing, the data subject should be able to "opt-out" from having his/her data used for such purposes at any stage'.[31]

23.37 There is a question whether the relevant privacy principle should adopt an opt-in regime, an opt-out regime, or neither. In other words, should organisations engaged in direct marketing be required to allow individuals to opt out of receiving direct marketing communications; should organisations only be permitted to engage in direct marketing if the individual in question has explicitly opted in to receiving such communications; or should neither of these requirements apply?

23.38 Assuming that either an opt-in or an opt-out model is adopted, a related question is whether direct marketers should be required to comply within a set timeframe. That is, when a person expresses their intention to opt out (or to refuse to opt in) to receiving direct marketing communications, should the organisation be required to comply with this request to be removed from a direct marketing list within a period specified in the privacy principle?

Submissions and consultations

23.39 A large number of stakeholders submitted that the direct marketing privacy principle should provide individuals with a general right to opt out of direct marketing communications at any time.[32] A number of stakeholders also suggested that organisations engaged in direct marketing should be obliged to comply with a request to be removed from a direct marketing list within a specified period.[33] One stakeholder suggested that, consistently with the *Spam Act*, this period should be within five business days of an individual's request.[34]

23.40 There was also some opposition to including a specific opt-out requirement in the relevant privacy principle. A number of stakeholders submitted that, where a

---

31 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998, Ch 1.

32 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; The Mailing House, *Submission PR 64,* 1 December 2006.

33 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007. One stakeholder submitted that organisations should be encouraged, rather than required, to do this: Veda Advantage, *Submission PR 163,* 31 January 2007.

34 Law Council of Australia, *Submission PR 177,* 8 February 2007.

business already has an opt-out policy for direct marketing, this is sufficient.[35] The ABA submitted that it might not be desirable to include a legislative requirement to provide such an opt-out mechanism, without first carefully analysing the benefits and disadvantages that this might have. It suggested, as an alternative, a requirement that an organisation notify 'the individual that personal information is being collected for the primary purpose of direct marketing and that it may also be disclosed to other organisations for that purpose'.[36]

23.41 At the other end of the spectrum, some stakeholders submitted that direct marketing should be permitted only if the individual has opted in to receiving such communications.[37] This could still be subject to exceptions that apply, for instance, to charitable organisations.[38] This was opposed by other stakeholders. For example, the Mailing House stated that 'any move to introduce an "opt in" rather than the existing "opt out" regime will have a huge adverse impact on business'.[39]

ALRC's view

23.42 There was relatively little support for adopting the most restrictive regulatory regime in the privacy principles for those engaged in direct marketing—an opt-in model. The ALRC believes that the fact that the *Spam Act* incorporates at least a modified form of opt-in model does not mean that this is necessarily appropriate for *all* forms of direct marketing in *all* contexts.[40] This view is consistent with the ALRC's earlier proposal that the privacy principle dealing with direct marketing should be of general application but, where different requirements are necessitated in certain specific contexts, separate sectoral legislation should be enacted to displace any of the general provisions in the relevant *Privacy Act* privacy principle.[41] It is entirely appropriate for such sectoral legislation to impose a different level of restriction—that is, more or less onerous—on those engaged in direct marketing.

23.43 As outlined above, the vast majority of stakeholders preferred that the *Privacy Act* adopt an opt-out model to regulate direct marketing. This support was expressed by a broad range of stakeholders, including individuals, some entities directly or indirectly involved in direct marketing, the OPC and privacy advocates. Nevertheless, some concern was expressed that an opt-out model would be too restrictive on businesses that use direct marketing to communicate with existing or potential customers.

23.44 It should be noted, however, that the bulk of submissions from the business community to the OPC Review were in favour of an opt-out model to regulate direct

---

35 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; ANZ, *Submission PR 173,* 6 February 2007.
36 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
37 See, eg, Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
38 Ibid.
39 The Mailing House, *Submission PR 64,* 1 December 2006.
40 The *Spam Act 2003* (Cth) is considered in greater detail in Part J of this Discussion Paper.
41 See Proposal 23–2.

marketing.[42] Moreover, concerns about an opt-out model may be overstated, given that NPP 2 already essentially provides for an opt-out model in respect of secondary purpose direct marketing, by providing that:

- an organisation engaged in secondary purpose direct marketing is prohibited from using or disclosing an individual's personal information if he or she has requested not to receive direct marketing communications from the organisation;[43] and

- in each direct marketing communication, an organisation must give the individual recipient the option of not receiving further direct marketing communications.[44]

23.45 As explained in the OPC Review, a *general* right to opt out of direct marketing would merely extend the existing opt-out model to apply to use and disclosure of personal information carried out for the *primary* purpose of direct marketing.[45] The ALRC favours this approach for two main reasons. First, it would increase individuals' control over their personal information without the significant compliance costs associated with a completely new collection and notification regime.[46]

23.46 Secondly, as noted above, one of the problems with the Act dealing with direct marketing in NPP 2.1(c) is that this principle only covers personal information collected for a *secondary* purpose of direct marketing. Proposal 23–1 above attempts to solve this problem by making the direct marketing rules apply irrespective of whether carrying out direct marketing is the collector's primary or secondary purpose.

23.47 There was a range of views on whether organisations engaged in direct marketing should be required to comply with a request not to receive direct marketing communications within a specified period. Some stakeholders clearly preferred either that no amount of days be specified, or that the obligation only be to comply within a 'reasonable' time.

23.48 There was also no consensus among those who specified a timeframe. One view was that any such timeframe should be consistent with the *Spam Act*, which provides for five business days within which to action the request.[47] On the other hand, in the OPC Review, the OPC described as 'consistent' with its own position the view

---

42 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 97–98.
43 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(c)(iii).
44 Ibid sch 3, NPP 2.1(c)(iv).
45 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 102.
46 A similar point was made, in relation to compliance costs, in Ibid, 102.
47 See *Spam Act 2003* (Cth) sch 2, cl 6(1).

expressed by the Australian Direct Marketing Association that the period should be 45 days.[48]

23.49 The ALRC's view is that, in order to make the opt-out model effective, it should provide that organisations must act on a request by an individual not to receive any further direct marketing communications within a reasonable period of time.

23.50 The ALRC acknowledges that the period of five business days, as provided for in the *Spam Act*, was based on a period that Parliament considered to be 'reasonable' in the context of communication by email.[49] This was the subject of a review by the Australian Government Department of Communications, Information Technology and the Arts, which found that this period was appropriate and ought not be amended.[50] The ALRC believes, however, that such a period may be too short, in light of the fact that a large proportion of direct marketing does not occur electronically, and so other factors (such as the delivery time of the postal service) need to be taken into account.

23.51 Moreover, in light of the wide variation in the timeframes suggested by stakeholders, the ALRC's present view is that the Act should not specify an amount of days within which to act on any request not to receive direct marketing communications. Rather, the organisation should comply within a reasonable time. The term 'reasonable' should be interpreted with reference to all relevant factors, including how the direct marketing communications are transmitted and the length of time it takes to amend an organisation's database.

Proposal 23–3 The proposed 'Direct Marketing' principle should require organisations to present individuals with a simple means to opt out of receiving direct marketing communications.

Proposal 23–4 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must comply, within a reasonable time, with an individual's request not to receive direct marketing communications.

48 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 100.

49 Explanatory Memorandum, Spam Bill 2003 (Cth), 11.

50 See Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006), 64, rec 10.

Other possible requirements

Original source of personal information

23.52 A number of other possible amendments to the rules on direct marketing have been suggested. The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to require organisations to take reasonable steps, on request, to advise an individual from where it acquired the individual's personal information.[51]

23.53 In its submission to the OPC Review, ADMA stated that the rationale behind such a provision is that 'informing individuals of the source of the data being used gives them more control over their personal information and reduces the number of repeat complaints about unsolicited marketing'.[52]

Submissions and consultations

23.54 A large number of stakeholders submitted that the Act should require organisations to take reasonable steps, on request, to advise an individual from where it acquired the individual's personal information.[53] This requirement would help an individual to take steps to have their contact details removed from a 'master list' that may be used by many other organisations involved in direct marketing.[54]

23.55 One individual explained the rationale as follows:

> Some marketing organisation has gotten my details for on-selling, but I can't get at the 'source'. I can only tell marketers who contact me directly to remove my name from their individual lists. I want for the 'source' to be obliged to tell me on a regular basis … what details they have on me, and give me the chance to have my details removed from their master list.[55]

23.56 ADMA agreed that this information should be provided by organisations making an unsolicited approach to individuals, but stated that the requirement should be stated in OPC guidelines, rather than in the Act, because it was concerned that

---

51 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 24.

52 Ibid, 101–102.

53 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Anonymous, *Submission PR 189,* 10 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. One stakeholder submitted that organisations should be encouraged, rather than required, to do this: Veda Advantage, *Submission PR 163,* 31 January 2007.

54 Anonymous, *Submission PR 189,* 10 February 2007.

55 Ibid.

'small organisations and charities do not have the technical capability to comply with such a requirement'.[56]

Particularly vulnerable individuals

23.57 Concerns have been raised about the practice of sending direct marketing communications to vulnerable people in the community. For example, direct marketing may pose a particular risk to children, young people and adults with a decision-making disability because their cognitive faculties may be less developed than other people, thus making it more likely that they will be manipulated by direct marketing. The Obesity Prevention Policy Coalition and Young Media Australia submitted that 'direct marketing of unhealthy food and beverages to children and young people may influence them to consume unhealthy foods, and contribute to them becoming overweight or obese'. Moreover, they submitted that 'children are more susceptible to commercial manipulation than adults'.[57]

23.58 These problems are exacerbated by factors including that children and young people often 'lack the cognitive capacity and maturity' to give informed consent, and also that new technologies (such as the internet, email and SMS) are increasingly being used in direct marketing to children. For this reason, it was submitted that organisations should be prohibited from engaging in direct marketing with a child under 14 years, unless a parent has provided 'express and verifiable consent'.[58]

23.59 Similarly, direct marketing can be insensitive where an error in a personal information database causes direct marketing communications to be sent, for instance, to a grieving friend or relative of a deceased individual. One individual stated that it can be traumatic to receive direct marketing communications addressed to her late husband, and this should be rectified by requiring organisations involved in direct marketing to update their databases regularly.[59] The ALRC Phone-In also received a number of calls stating that direct marketing can be frightening for older people.

23.60 The question arises whether reform is desirable to address these issues. If so, should the reform be carried out at the level of the privacy principles or in guidance issued by the OPC?

ALRC's view

23.61 As noted above, a very large number of submissions to this Inquiry were in favour of requiring organisations involved in direct marketing to take reasonable steps, on request, to advise an individual from where it acquired the individual's personal information.

---

56 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007.
57 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.
58 Ibid.
59 A Baxter, *Submission PR 74,* 5 January 2007.

23.62 Such a requirement would be particularly useful where an individual's personal information has been disclosed by an organisation to another organisation and it has then been used to carry out direct marketing. In such a situation, the individual could follow a 'chain' of disclosure to the original source and, if he or she wished, the individual could then take action to have his or her name removed from the list. This would facilitate individuals being able to assert substantive, as distinct from merely formal, privacy rights with respect to direct marketing.

23.63 Such a requirement would have the further benefit of encouraging organisations to consider whether they have a legitimate basis for collecting the personal information in the first place. For example, an organisation may be more likely to consider whether it would contravene the collection principle for it to collect personal information about an individual (X) from a third person (Y) where the organisation knows, or reasonably suspects, that X did not willingly provide the personal information to Y.

23.64 For these reasons, the ALRC believes it would be desirable to require organisations involved in direct marketing to take reasonable steps, on request, to advise an individual from where it acquired the individual's personal information.

23.65 The second question is whether reform is needed to address the particular needs of vulnerable individuals. The ALRC recognises that children, young people and adults with a decision-making disability can be particularly at risk from direct marketing. To the extent that such individuals have diminished capacity to exercise independent judgment in respect of the matters raised in direct marketing communications to him or her, organisations should be discouraged from making the communication in the first place. Nevertheless, the ALRC's view is that a change to the relevant privacy principle would likely be a blunt instrument to achieve such a result, and it may have undesirable consequences in denying such a person's ability to make decisions as to his or her own privacy. Instead, the ALRC proposes that the OPC issue guidance to help organisations better understand how to communicate fairly by way of direct marketing to such individuals, and when it is inappropriate to do so. In particular, this guidance should help to clarify organisations' obligations in dealing with particularly vulnerable people, such as elderly individuals and individuals aged 14 and under.[60]

23.66 Where communication by direct marketing can itself be traumatic—for example, as in the situation described above, communication addressed to a deceased individual and received by that individual's grieving friend or relative—the ALRC believes that the issue relates most directly to the data quality principle. As set out in Chapter 24, the ALRC proposes that all personal information that is collected, used or disclosed by an organisation should be 'accurate, complete, up-to-date and relevant'. The ALRC's view is that the OPC should issue guidance to organisations engaged in

---

60 Dealing with individuals aged 14 and under is discussed in greater detail in Ch 60.

direct marketing to highlight these obligations and assist them with information on how best to fulfil them.

Proposal 23–5 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must, when requested by an individual to whom it has sent direct marketing communications, take reasonable steps to advise the individual from where it acquired the individual's personal information.

Proposal 23–6 The Office of the Privacy Commissioner should issue guidance to organisations involved in direct marketing, which should:

(a) highlight their obligation to maintain the quality of any database they hold containing personal information and assists them in achieving this requirement; and

(b) clarify their obligations under the *Privacy Act* in dealing with particularly vulnerable people, such as elderly individuals and individuals aged 14 and under.

Summary of proposed 'Direct Marketing' principle

23.67 In summary, the ALRC's view is that the sixth principle in the proposed UPPs should be called 'Direct Marketing'. It should appear as follows.

UPP 6. Direct Marketing (only applicable to organisations)

6.1 An organisation must not use or disclose personal information about an individual for the primary purpose or a secondary purpose of direct marketing unless all of the following conditions are met:

(a) the individual has consented, or both of the following apply:

(i) the information is not sensitive information; and

(ii) it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and

(b) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(c) the individual has not made a request to the organisation not to receive direct marketing communications, and the individual has not withdrawn any consent he or she may have provided to the organisation to receive direct marketing communications; and

(d) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(e) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be contacted directly electronically.

6.2 In the event that an individual makes a request of the organisation not to receive any further direct marketing communications, the organisation must comply with this requirement within a reasonable period of time.

6.3 An organisation must take reasonable steps, when requested by an individual to whom it has sent direct marketing communications, to advise the individual from where it acquired the individual's personal information

24. Data Quality

Contents

Introduction 719
Application of data quality principle to agencies 720
Submissions and consultations 720
ALRC's view 721
Scope of data quality principle 721
Background 721
Submissions and consultations 722
ALRC's view 724
Clarification of data quality principle 726
Submissions and consultations 726
ALRC's view 727
Summary of proposed 'Data Quality' principle 727

Introduction

24.1 The *Privacy Act 1988* (Cth) contains provisions that are designed to ensure that, where an agency or organisation handles personal information, it takes reasonable steps to ensure that the information is of a sufficiently high 'quality'. These are commonly known as 'data quality' requirements. Ensuring that personal information that is collected, used and disclosed is, among other things, accurate has long been seen as a fundamental obligation of data collectors operating under the *Privacy Act*.[1]

24.2 The National Privacy Principles (NPPs) require an organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.[2] A similar provision is contained in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines).[3]

---

1 See, eg, Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General), 2117; Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 141.

2 *Privacy Act 1988* (Cth) sch 3, NPP 3.

3 See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.

24.3 By contrast, the Information Privacy Principles (IPPs) do not contain a 'stand-alone' data quality principle. Aspects of the data quality principle can be found in IPPs 3 and 8. IPP 3 provides that, where personal information is solicited by the collector, the collector must take reasonable steps to ensure the information is relevant to the purpose of collection, up-to-date and complete. IPP 8 provides that, before a data collector proposes to use personal information, it should take reasonable steps to ensure the information is accurate, up-to-date and complete.

24.4 In other words, there appears to be a gap in the IPPs in that they do not impose data quality requirements at the time of disclosure. This differs from some overseas legislation. For example, US privacy legislation requires government agencies to ensure that, before disclosing a record about an individual to any person other than an agency, they make reasonable efforts to ensure that such records are 'accurate, complete, timely and relevant for agency purposes'.[4]

24.5 This chapter considers three main questions. First, should the proposed Unified Privacy Principles (UPPs) contain a single data quality principle that covers both agencies and organisations?[5] Secondly, assuming that such a principle is adopted, what should be the scope of the proposed 'Data Quality' principle? Thirdly, is it necessary to clarify any of the provisions relating to data quality that the ALRC proposes to retain?

Application of data quality principle to agencies

24.6 As noted above, agencies and organisations are currently subject to similar, but subtly differing, requirements in relation to data quality. In Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether agencies should be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information.[6]

Submissions and consultations

24.7 A number of stakeholders submitted that agencies should be subject to the same stand-alone data quality principle as organisations.[7] Reasons advanced in favour of this argument include that this would provide a 'clear and unambiguous' framework 'promot[ing] better compliance, as well as greater public confidence in the agencies'.[8]

---

4 *Privacy Act 1974* 5 USC § 552a (US). There is an exception to this requirement. See also G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, Principle 10.

5 The ALRC proposes to consolidate the IPPs and NPPs to create a single set of privacy principles, the UPPs, that would be generally applicable to agencies and organisations: see Proposal 15–2.

6 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–16.

7 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; CrimTrac, *Submission PR 158,* 31 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

8 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

It was also suggested that this would help provide a more consistent approach to maintaining data quality as between organisations and agencies.[9]

24.8 Some stakeholders submitted that it was unnecessary to make agencies subject to a discrete data quality principle.[10] The Australia Federal Police simply stated that 'IPP 8 is sufficient'.[11]

ALRC's view

24.9 The majority of stakeholders that commented on this issue supported moving to a single privacy principle dealing with data quality. This principle should be applicable to agencies and organisations. The ALRC supports this reform and notes that this is consistent with Proposal 15–2 to move to a single set of privacy principles, the UPPs.

24.10 The ALRC believes this reform would also be beneficial in consolidating and simplifying the existing provisions of the IPPs and NPPs that deal with data quality. As noted above, NPP 3 deals with the issue of data quality identically in respect of all of the most important stages of the information cycle—namely, collection, use and disclosure. On the other hand, the IPPs cover these stages only partially and there are some subtle differences between the obligations at different stages. This can cause confusion and can undermine the integrity of information management systems.

24.11 The ALRC believes, therefore, that consolidating the data quality obligations applicable to agencies and organisations in a single privacy principle will encourage better handling of personal information by agencies and organisations.

Proposal 24–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Data Quality' that applies to agencies and organisations.

Scope of data quality principle

Background

24.12 In IP 31, the ALRC asked what should be the scope of the data quality principle.[12] A specific issue was whether it is desirable to extend the reach of NPP 3 to apply expressly to personal information that an organisation controls, which may not

9 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
10 Queensland Government, *Submission PR 242,* 15 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; AXA, *Submission PR 119,* 15 January 2007.
11 Australian Federal Police, *Submission PR 186,* 9 February 2007.
12 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–14.

necessarily be information that the organisation has in its direct possession. Unlike NPP 3, IPP 8 imposes express obligations in relation to data quality on a record-keeper who has 'possession or control' of a document.[13]

24.13 Another issue was whether the data quality principle should include the requirement that the information be relevant; a requirement not currently included in NPP 3. This differs from the OECD Guidelines,[14] the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive),[15] and some state and territory legislation, such as the *Personal Information Protection Act 2004* (Tas).[16] For example, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under art 29 of the EU Directive, summarised as a core principle in the EU Directive that

> data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.[17]

24.14 In contrast, NPP 1 (the collection principle) provides that, at the stage of collection, personal information must be necessary for one or more of the organisation's functions or activities. The IPPs contain an express provision stating that, at the time of collection, personal information must be relevant to the purpose of collection.[18] There is also a stand-alone IPP requiring that personal information be used only for relevant purposes.[19]

Submissions and consultations

Possession or control

24.15 A number of stakeholders submitted that the data quality principle should apply to personal information that is in the 'possession or control' of agencies and organisations.[20] The Office of the Victorian Privacy Commissioner noted that this

---

13 Similarly, *Privacy Act 1988* (Cth) s 18G, imposes obligations relating to data quality on a credit reporting agency in 'possession or control' of a credit information file, and on a credit provider or credit reporting agency in 'possession or control' of a credit report.

14 See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.

15 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 6.

16 See *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 3.

17 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998.

18 *Privacy Act 1988* (Cth) s 14, IPP 3(c).

19 Ibid s 14, IPP 9.

20 Government of South Australia, *Submission PR 187,* 12 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

obligation applies under Victorian privacy law.[21] Some organisations noted that, as a matter of good business practice, they commit to ensuring that information held about their customers is accurate, complete and up-to-date.[22]

24.16 On the other hand, some stakeholders argued that it would be problematic to extend the principle to personal information in the *control*, but not necessarily the possession, of the data collector. Some argued that this would create additional 'complexity and uncertainty'.[23] Where an organisation (X) outsources its activities to another organisation (Y), it may become unclear as to whether the data in question remain under X's control.[24] Professor William Caelli rejected this argument, however, stating that X remains 'responsible' for the integrity of the data even if it chooses to outsource the collection (or other handling) of the data to Y.[25]

24.17 The Australian Government Department of Health and Ageing argued that the critical factor should not be whether the data are in the control of the agency or organisation, but whether the data are to be used or disclosed.[26] A similar point was made by the Office of the Privacy Commissioner (OPC), which argued that the obligation should only apply to persons that are collecting, using or disclosing data, as distinct from merely controlling data. To impose the data quality requirements on all entities that control personal information would extend the requirement to entities that merely hold a copy of the information in question on behalf of someone else.[27]

Criteria in the data quality principle

24.18 All the stakeholders who commented on this issue submitted that the data quality principle should include the requirement that the information be relevant to a permitted purpose of collection, use or disclosure.[28]

24.19 Other stakeholders suggested refinements to the scope and criteria of the data quality principle. AXA suggested that the principle should apply with reference to the purpose for which the information is held. For example, if it is necessary to hold certain information as a historical record, the requirement that data be kept 'up-to-date' should not apply.[29] A number of stakeholders stressed the importance of retaining the

---

21 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
22 See, eg, AAMI, *Submission PR 147,* 29 January 2007.
23 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.
24 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
25 W Caelli, *Submission PR 99,* 15 January 2007.
26 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.
27 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
28 Ibid; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
29 AXA, *Submission PR 119,* 15 January 2007.

qualification in NPP 3 that states that a data collector need only take 'reasonable steps' to maintain data quality.[30] The OPC emphasised that the data quality principle should not be interpreted as a requirement for a data collector 'constantly [to] contact individuals to ensure information is accurate'.[31]

ALRC's view

Possession or control

24.20 As noted above, the data quality obligations in NPP 3 apply only when the data collector collects, uses or discloses personal information. There was considerable disagreement among stakeholders as to whether these requirements should apply also when a data collector merely controls the information.

24.21 The ALRC shares the concern of a number of stakeholders that such an extension would impose the data quality requirements to a broader class of persons than is reasonable or necessary to protect individuals' information privacy. For example, where an organisation maintains a database containing personal information on behalf of another organisation, it would be very onerous—and often unreasonable—to expect the second organisation to maintain the data quality of the personal information in the database. The ALRC, therefore, believes that extending the data quality principle in this way would impose an unjustified compliance burden on agencies and organisations.

Additional criterion: relevance

24.22 The ALRC shares the view of stakeholders that the 'Data Quality' principle in the proposed UPPs should require that, where an agency or organisation collects, uses or discloses personal information, the information should be relevant to the purpose for which it was collected or a permitted secondary purpose. This complements the requirement in NPP 1.1 that personal information collected by an organisation should be 'necessary for one or more of its functions or activities'.[32] If the purpose of collection is not necessary for one or more of the data collector's functions or activities, the requirement in NPP 1.1 cannot be satisfied. It is logical, therefore, to include a corresponding obligation to limit the use and disclosure of personal information to that which is relevant to a purpose permitted under the privacy principles.

24.23 Moreover, the ARLC believes that the fact that an agency or organisation has legitimately collected personal information for a permitted purpose should not mean that it is necessarily allowed to use or disclose *all* of that information, in the event that

---

30 See, eg, G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

31 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

32 The ALRC's view is that this requirement should be retained, in a modified form, in the proposed UPPs: see Proposal 18–3. See also the similar provision in *Privacy Act 1988* (Cth) s 14, IPP 1.1(b).

its proposed use or disclosure is permitted under the privacy principles. Rather, the agency or organisation should be allowed to use or disclose only so much of the personal information it holds as is relevant to a purpose permitted by the privacy principles.

24.24 This is illustrated by the following hypothetical example. Imagine that a company, X, lawfully collected personal information about an individual, Y, including her address, job description, marital status, physical disabilities and financial position. This was necessary for the purpose of providing Y with financial advice. Some time later, X wishes to disclose Y's personal information to another company, Z, for the purpose of buying shares on Y's behalf—this being a related secondary purpose that Y would reasonably expect. Common sense dictates that X should not be permitted to disclose to Z *all* the personal information it holds on Y. Instead, X should be allowed to disclose only such personal information about X as is relevant to the permitted secondary purpose of obtaining the shares.

24.25 It is arguable that such a requirement is already implicit in the NPPs. However, given that the IPPs expressly mention relevance, but the NPPs do not, it is desirable to avoid all doubt by adding the criterion of relevance to the 'Data Quality' principle in the proposed UPPs.

Reference to permitted purpose

24.26 A number of stakeholders identified that the criteria by which the data quality principle operates—in NPP 3, these criteria are that the personal information must be 'accurate, complete and up-to-date'—are not self-evidently clear. For example, on one view, a document that contains personal information about an individual in 1990 might no longer be 'accurate' or 'up-to-date' in 2007. Nevertheless, there might be a valid reason not to update the document if it is necessary to maintain a historical record.

24.27 The ALRC agrees that the above criteria may be ambiguous and that it would be desirable to make clear that they should be understood with reference to the purpose for which the personal information was collected, or another purpose permitted under the privacy principles. This is consistent with the OECD Guidelines, which provide that:

> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[33]

33 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.

Proposal 24–2 The proposed 'Data Quality' principle should require an agency or organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the proposed UPPs, accurate, complete, up-to-date and relevant.

Clarification of data quality principle

24.28 One issue raised in the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) concerned the interpretation of NPP 3. Some organisations consider that their obligations under NPP 3 to keep personal information up-to-date and accurate are absolute, and could be used to justify intruding upon an individual's privacy.[34] The OPC stated that it is not 'reasonable' to take steps to ensure data accuracy where this has no privacy benefit for the individual. It said that legislative amendment of NPP 3 was unnecessary but indicated that it would issue further guidance to organisations about their obligations under NPP 3 to ensure a proportional approach is taken to compliance.[35]

24.29 Canadian privacy legislation, for example, is clear that the obligation to maintain data quality is qualified.[36] Similarly, the Data Quality Principle in the OECD Guidelines qualifies the requirement that personal data be accurate, complete and up-to-date, by stating that the requirement only arises to the extent necessary for the purposes for which the data are to be used.

24.30 The ALRC asked in Question 4–15 of IP 31 whether guidance by the OPC is an appropriate and effective response to this issue, or whether it would be more appropriate to amend the relevant privacy principle.

Submissions and consultations

24.31 A large number of stakeholders suggested that the data quality principle does not require expansion to set out in greater detail what is required; instead, guidance from the OPC would be sufficient.[37] Concern was expressed that legislative

---

34 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 267–268.

35 See Ibid, rec 79.

36 See *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch, Principle 4.6, and discussion below on Canadian principles.

37 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,*

amendment may lead to further confusion.[38] It was also suggested that the current provision allows a more flexible response to new technologies.[39] While supporting the provision of 'regular and detailed' guidance by the OPC, based on the guidelines provided by the National Institute of Science and Technology in the United States, one submission argued that this obligation on the OPC should be stated in the data quality principle.[40] The Centre for Law and Genetics submitted that explicit guidance in the principle would remove doubt on this issue.[41]

ALRC's view

24.32 A very large number of stakeholders submitted that it was unnecessary to amend the relevant privacy principle to make clear that there is no absolute obligation to ensure that personal information is up-to-date and accurate; only one submission favoured such an amendment to the privacy principle. This indicates a general consensus that there is not widespread concern that the data quality principle is ambiguous or unclear in this way.

24.33 The ALRC shares the view that it is unnecessary to include a provision in the proposed 'Data Quality' principle explicitly stating that the obligations are not absolute. As noted by some stakeholders, such an amendment runs the risk of causing more confusion than it resolves. In coming to this view, it is noted that the OPC has already undertaken to provide further guidance on this issue and the ALRC is of the opinion that this guidance would constitute a sufficient response.

Summary of proposed 'Data Quality' principle

24.34 In summary, the ALRC's view is that the seventh principle in the proposed UPPs should be called 'Data Quality'. It should appear as follows.

---

15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

38 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

39 CSIRO, *Submission PR 176,* 6 February 2007.

40 W Caelli, *Submission PR 99,* 15 January 2007.

41 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

UPP 7. Data Quality

An agency or organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the UPPs, accurate, complete, up-to-date and relevant.

25. Data Security

Contents

Introduction 729
Current coverage by IPPs and NPPs 731
Towards a single data security principle 731
ALRC's view 732
Protection of personal information 733
Background 733
Submissions and consultations 734
ALRC's view 737
Destruction versus retention of personal information 739
ALRC's view 740
Extension of destruction and de-identification requirements to agencies 741
Background 741
Submissions and consultations 742
ALRC's view 743
When is destruction or deletion appropriate? 745
Background 745
Submissions and consultations 746
ALRC's view 747
General right to destruction of personal information? 748
Submissions and consultations 748
ALRC's view 749
Meaning of 'destroy or permanently de-identify' 750
Submissions and consultations 750
ALRC's view 751
Summary of proposed 'Data Security' principle 753

Introduction

25.1 The *Privacy Act 1988* (Cth) requires that agencies and organisations take reasonable steps to maintain the security of personal information that they hold. This is commonly referred to as 'data security' and it involves protecting personal information in two main ways: preventing misuse and loss; and destroying or permanently de-

identifying personal information that is no longer needed for a purpose permitted by the privacy principles.[1]

25.2 In order to comply with their data security obligations, agencies and organisations must institute measures that deal with matters including: how and where personal information is physically stored; the security of electronic records; staff access to records; the transfer of personal information; and the destruction of personal information.[2]

25.3 The privacy laws of a number of other jurisdictions also contain provisions relating to data security that apply both to public and private sector entities. For example, United Kingdom data protection law states:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[3]

25.4 Similarly, Part I of the *Federal Data Protection Act 1990* (Germany), which applies to both the public and private sectors, contains technical and organisational requirements to combat unauthorised access to personal data.[4] This is a manifestation of the Security Safeguards Principle in the Organisation for Economic Co-operation and Development's *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002) (OECD Guidelines). It also responds to the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive), which provides that

> technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.[5]

25.5 This chapter covers the following main issues. First, it considers whether the proposed Unified Privacy Principles (UPPs) should contain a single data security principle that covers both agencies and organisations.[6] Secondly, the chapter addresses how agencies and organisations should fulfil their data security obligations. Thirdly,

---

1 It should be noted that the ALRC proposes that, where the *Privacy Act* uses the term 'de-identify', this should be amended to read 'render non-identifiable': see Ch 3. For the purposes of this chapter, this change in terminology is adopted only in the relevant proposals and in the 'Data Security' principle in the proposed Unified Privacy Principles. To avoid confusion and for ease of reference the text of this chapter generally continues to use the term 'de-identify'.

2 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–3010].

3 *Data Protection Act 1998* (UK) s 5, Principle 7.

4 *Federal Data Protection Act 1990* (Germany) s 9, Annex.

5 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 17.

6 The ALRC proposes to consolidate the IPPs and NPPs to create a single set of privacy principles, the UPPs, which would be generally applicable to agencies and organisations: see Proposal 15–2.

the chapter considers the content and application of the requirement to destroy or permanently de-identify personal information held by agencies and organisations.

Current coverage by IPPs and NPPs

25.6 The Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) both contain provisions dealing with data security. IPP 4 provides that a record-keeper, who has possession or control of a record that contains personal information, must ensure that:

- the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and

- if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of the information contained in the record.

25.7 An agency can breach the principle if it fails to have reasonable security safeguards in place, even if no loss or unauthorised access or disclosure takes place.[7]

25.8 NPP 4 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure. In addition, an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2. The OPC has provided guidance on an organisation's obligations in relation to physical security, computer and network security, communications security and personnel security.[8]

Towards a single data security principle

25.9 As noted above, agencies and organisations are subject to data security requirements under the IPPs and NPPs respectively. However, those principles differ subtly. There is a question whether these differences should be reconciled with a view to creating a single data security principle that is applicable to agencies and organisations.

---

7 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998).

8 See Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001).

25.10 Although this question was not asked explicitly in the ALRC's Issues Paper, *Review of Privacy* (IP 31), it was implied in the questions dealing with specific aspects of the data security principles in IPP 4 and NPP 4.[9] Moreover, any answer to this general question has ramifications for the ALRC's proposal to adopt a single set of privacy principles, the UPPs, covering both agencies and organisations.[10]

25.11 Consequently, while most stakeholders did not state their views on whether IPP 4 and NPP 4 should be consolidated,[11] it should be noted that a consistent theme in submissions and consultations was the importance of creating clear and broadly applicable data security provisions, particularly given the risks posed by identity theft, among other problems.[12]

ALRC's view

25.12 The ALRC's view is that there should be a single data security principle that is applicable to agencies and organisations. Such a reform is consistent with Proposal 15–2 to adopt a single set of privacy principles that binds agencies and organisations.

25.13 The ALRC also believes that this would be beneficial in consolidating and simplifying the existing provisions of the IPPs and NPPs that deal with data security. As discussed later in this chapter, there are a number of gaps and inconsistencies as between the IPPs and NPPs. Provided the UPP dealing with data security is sufficiently flexible to accommodate the differences between the operation of the public and private sectors, the ALRC can see no good policy reason to maintain two separate principles dealing with data security.

Proposal 25–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Data Security' that applies to agencies and organisations.

---

9 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–17, 4–18 and 4–19.

10 See Proposal 15–2.

11 It should be noted, however, that the OPC specifically submitted that such a consolidation should occur: Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

12 See, eg, National Association for Information Destruction, *Submission PR 133,* 19 January 2007; W Caelli, *Submission PR 99,* 15 January 2007. Note, also, that identity theft is discussed in greater detail in Ch 9.

Protection of personal information

Background

Disclosure of personal information to contractors

25.14 Unlike NPP 4, IPP 4 expressly obliges a record-keeper to take reasonable steps to prevent unauthorised use or disclosure of personal information contained in a record where it is necessary for the record to be given 'to a person in connection with the provision of a service to the record-keeper'.[13] There is a question whether the data security privacy principle should require organisations, as well as agencies, to ensure the protection of personal information they disclose to contractors.[14]

25.15 One advantage of making specific provision in this area is that it would overcome some of the problems that arise where an organisation engages in outsourcing—for example, where an organisation subcontracts to an entity that is not covered by the *Privacy Act*. The Office of the Privacy Commissioner (OPC) responded to the problem of outsourcing by issuing guidance, stating that 'where there is a particularly close relationship between an organisation and a contractor it may mean that the actions of the contractor could be treated as having been done by the organisation'.[15] In the specific context of an organisation that contracts with an entity that is subject to the small business exemption, the OPC stated:

> If an organisation is contracting with a business that is not covered by the *Privacy Act* it would be advisable to encourage the contractor to opt in to being covered… One way of doing this would be to make opting in a condition of the contract.
>
> Another less effective option would be for the organisation to have terms and conditions in the contract. These would bind the contractor to taking steps necessary to protect the personal information it holds that would be equivalent to the steps required by the NPPs.[16]

25.16 In 2005, the OPC recommended that the Australian Government consider amending NPP 4 to require organisations to ensure the protection of personal information they disclose to contractors.[17] German privacy law, for example, has a provision imposing a number of obligations on public and private bodies that

---

13 *Privacy Act 1988* (Cth) s 18G imposes similar security obligations on credit reporting agencies and credit providers in respect of credit files and reports given to persons in connection with the provision of a service to those agencies or providers. Credit reporting is dealt with in detail in Part G.

14 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–17.

15 Office of the Federal Privacy Commissioner, *Contractors*, Information Sheet 8 (2001).

16 Ibid. Note, however, that the ALRC proposes to remove the small business exemption from the Act: see Ch 35.

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 54. See also rec 56, which states that the OPC should issue guidelines to clarify that businesses, which give personal information to contractors, should impose contractual obligations on any contractors to take reasonable steps to protect the information.

commission agents to collect, process or use personal data. In particular, responsibility for compliance with data protection provisions rests with the principal body.[18]

The 'reasonable steps' requirement

25.17 A further question arises as to what an organisation should be required to do to satisfy the requirement that it has taken 'reasonable steps' in ensuring data security. This question arises in two related contexts. First, under NPP 4.1, an organisation is obliged to take 'reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure'. Secondly, IPP 4(a) imposes a similar requirement on agencies to ensure that a record containing personal information is protected 'by such security safeguards as is reasonable in the circumstance'.

25.18 The issue boils down to the following question: is it necessary to provide further explanation about what is involved in the requirement to take 'reasonable steps' in these contexts and, if so, should this be set out in the relevant privacy principle or elsewhere?

Submissions and consultations

Disclosure of personal information to contractors

25.19 A large number of stakeholders supported amending the data security principle to clarify that organisations, as well as agencies, must take reasonable steps to ensure that personal information they disclose to contractors is protected.[19] While stating its general position that the *Privacy Act* already provides that the organisation *and* any contractor is each separately responsible for meeting obligations under the Act, the OPC noted some situations where the first organisation (as distinct from the contractor) should be solely responsible:

- where the service organisation is behind the scenes, and its role in relation to the handling of personal information is constrained by a contract, it may be confusing and costly without any increase in privacy protection, for it to provide a separate notice to individuals
- if the service organisation is a small business operator, and therefore outside the Privacy Act's jurisdiction, individuals may have no choice about whether their information is provided to a service organisation, and no redress to either party

---

18 See *Federal Data Protection Act 1990* (Germany) s 11.

19 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

- some organisations prefer to 'brand' all activities even those they contract out so that they present one face to the customer.[20]

25.20 The OPC suggested the enactment of provisions equivalent to ss 12 and 95B of the *Privacy Act* to ensure that: (1) an organisation 'has obligations in relation to personal information over which it wishes to retain control regardless of where it is held'; and (2) 'both parties continue to have obligations when handling the information'.[21]

25.21 The Australian Bankers' Association argued, however, that amending the data security principle is unnecessary in light of the OPC's Information Sheet 8 (discussed above), because it already provides guidance to an organisation on how to protect the security of personal information handled by a contractor.[22] On the other hand, a number of stakeholders have specifically complained about the lack of clarity as to what is required by the current requirement to 'take reasonable steps' to protect personal information, where there is only limited guidance from the OPC.[23]

25.22 Other stakeholders submitted that the existing provisions of the *Privacy Act* were sufficient to protect personal information that is handled by third parties pursuant to outsourcing arrangements.[24] Some stakeholders noted that they already use contracts to require contractors to abide by the privacy policies of the head organisation.[25] AAMI stated that, if a data breach affecting a customer is caused by a contractor, the customer may complain using AAMI's internal dispute resolution process.[26]

25.23 Finally, some stakeholders proposed particular data security principle models. One suggestion was an amalgam of the relevant principles in the Asia-Pacific Privacy Charter and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[27] Microsoft Australia suggested that organisations should be required to 'develop, implement and maintain an information security program that contains appropriate administrative, technical and physical safeguards'. It submitted that a suitable model would be the United States *Gramm-Leach-Bliley Act 1999* (US).[28]

---

20 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

21 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A similar view was expressed by other stakeholders, including: NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

22 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

23 See, eg, National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

24 See, eg, AXA, *Submission PR 119,* 15 January 2007.

25 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

26 AAMI, *Submission PR 147,* 29 January 2007.

27 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

28 Microsoft Australia, *Submission PR 113,* 15 January 2007.

The 'reasonable steps' requirement

25.24 A large number of stakeholders supported the provision of further guidance as to the meaning of 'reasonable steps'. Several suggestions were made, including:

- Organisations could comply with an obligation to take responsible steps to ensure that personal information they disclose to contractors is protected by including appropriate terms in the contract between the organisation and its contractor.[29]

- The term 'reasonable' should be judged against a number of factors. Professor William Caelli suggested that those factors should be 'the current and likely threat situation' and 'the known vulnerability' of the communication medium.[30] In addition to these factors, Microsoft Australia added: the relative 'sensitivity' of the information; the current state of the art; and the cost of implementing the relevant measures.[31]

- An organisation should educate its staff and contractors appropriately in how to protect data security.[32] The New South Wales Disability Discrimination Legal Centre added that measures need to be taken to ensure that *former* staff also maintain confidentiality of personal information.[33]

25.25 The National Association for Information Destruction, Australian Members and Stakeholders Working Group (NAIDWG), submitted that Australia is '"out of step" with comparable international jurisdictions' because it provides insufficient guidance and, as a result, Australia possesses 'the weakest form of regulatory control for secure document destruction'.[34] It noted that § 682.3 of the *Fair Trade and Accurate Credit Transactions Act 2003* (US) imposes a 'reasonable measures' standard, which provides a number of examples of how to comply. They include:

> (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
>
> (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
>
> (3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction …

---

29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
30 W Caelli, *Submission PR 99,* 15 January 2007.
31 Microsoft Australia, *Submission PR 113,* 15 January 2007.
32 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.
33 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.
34 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

ALRC's view

Disclosure of personal information to contractors

25.26 The vast majority of stakeholders that commented on this issue were in favour of requiring agencies and organisations to take reasonable steps to ensure the protection of personal information they disclose to contractors. This would involve extending the requirement in IPP 4(a) that applies to agencies, so that it is also applicable to organisations.

25.27 The ALRC's view is that such an extension is desirable for three main reasons. First, the wording of NPP 4.1 has been widely criticised as ambiguous. It should be noted that one stakeholder submitted that NPP 4, when combined with the OPC's guidance in Information Sheet 8, is sufficiently clear as to the requirements on an agency in respect of personal information that is disclosed to contractors. This position is undermined, however, by the fact that, since it issued Information Sheet 8, the OPC has recommended that consideration be given to amending the data security principle to require organisations to protect the personal information they disclose to contractors.[35]

25.28 Secondly, this reform would give clearer effect to the intended operation of NPP 4.1, as evidenced by Information Sheet 8, and bring the 'Data Security' principle in the proposed UPPs into line with IPP 4(b). In this way, it would not constitute a significant compliance burden for organisations, and particularly for those that are already contractually required to comply with the IPPs.

25.29 Thirdly, this amendment is consistent with the ALRC's view that a number of exemptions should be removed from the *Privacy Act*, including the small business exemption.[36] Clarifying that agencies and organisations must take reasonable steps to ensure that contractors protect personal information reflects that there are very few situations, if any, when contractors should be permitted to operate without reference to individuals' information privacy.

The 'reasonable steps' requirement

25.30 A related question arises as to the meaning of the term 'reasonable steps' in this context. The ALRC received a number of suggestions about how agencies and organisations should be required to satisfy this requirement. As a general proposition, the ALRC believes that the term 'reasonable steps' should not be expanded upon in the proposed UPPs, which are intended to be simple, high-level and of general

---

35 See Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 54.

36 See Part E.

application.[37] Moreover, further statutory elucidation is unnecessary given other requirements in the proposed UPPs—for example, the requirement for an agency or organisation to create a Privacy Policy that outlines how it proposes to handle personal information consistently with the *Privacy Act*.[38]

25.31 Instead, the ALRC believes that the OPC should provide guidance on the meaning of the term 'reasonable steps' in this context. That guidance could usefully include the following matters:

- An agency or organisation should frame its contract with a contracted service provider in such a way as to require the contracted service provider to handle any personal information disclosed to it in a manner that is consistent with the proposed UPPs.

- The OPC should provide guidance as to the impediments and assistance that can be obtained from new technology to ensure protection of personal information.[39]

- An agency or organisation should be encouraged to train its staff adequately on the steps they should take to protect personal information in the possession or control of the agency or organisation.

Proposal 25–2 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

Proposal 25–3 The Office of the Privacy Commissioner should provide guidance about the meaning of the term 'reasonable steps' in the context of the proposed 'Data Security' principle. Matters that could be dealt with in this guidance include:

(a) the inclusion of contractual provisions binding a contracted service provider of an agency or organisation to handle personal information consistently with the UPPs;

(b) technological developments in this area and particularly in relation to relevant encryption standards; and

37 See Proposal 15–1 and accompanying text.
38 See Ch 21.
39 The impact of developing technologies on privacy is discussed in detail in Part B.

(c) the importance of training staff adequately as to the steps they should take to protect personal information.

Destruction versus retention of personal information

25.32 Sometimes privacy law requires an agency or organisation that has collected personal information to destroy, delete or de-identify that information after a set period or in certain circumstances. This requirement may arise where, for example, an organisation has collected personal information for the specific purpose of identifying an individual. When the identification process has been completed, the organisation may no longer have a lawful purpose to hold the personal information and, as a result, the destruction or de-identification of the information may be the most effective means of protecting the individual against a subsequent misuse or unauthorised disclosure.

25.33 Section 18F of the *Privacy Act* provides an example of a legislative requirement to delete personal information in the specific context of credit reporting. German privacy law also requires private sector bodies to erase any data concerning 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life, criminal or administrative offences' where the data controller cannot prove that the data are correct.[40] The obligation is not dependent on a request being made by the individual concerned.

25.34 Conversely, sometimes privacy law imposes the opposite obligation—that is, an agency or organisation that has collected personal information may be obliged to *retain* that information for a minimum period or in certain circumstances. Arguably, this can give an individual more control over his or her personal information if the information is held in a central repository to which the individual has a right of access.

25.35 The requirement to retain personal information arises frequently in the context of health care and research. This is because retention of the data facilitates future care and research, given that there is often a long period between when the data are collected and when they may be of use.[41] For example, the 'data security and data retention' principle in Victorian health privacy law limits the circumstances in which a health service provider can delete information, and sets out certain procedures to be followed where deletion is allowed.[42] There is no equivalent provision in NPP 4 or

---

40 *Federal Data Protection Act 1990* (Germany) s 35(2).

41 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; CSIRO, *Submission PR 176,* 6 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

42 See *Health Records Act 2001* (Vic) sch 1, Health Privacy Principles 4.2, 4.3. These procedures involve the making of a written note of the person to whom the deleted information related, the period covered by the information and the date of deletion. This is discussed further in Part H.

IPP 4. In Victoria, deletion of health information relating to an individual is not permitted even if it is later found or claimed to be inaccurate, unless:

> (a) the deletion is permitted, authorised or required by the regulations or any other law; or
>
> (b) the deletion is not contrary to the regulations or any law and occurs:
>
> (i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or
>
> (ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider—
>
> whichever is the later.[43]

25.36 Other examples of where there is a need to preserve, rather than destroy, personal information is under general archives legislation[44] and, more specifically, in the child welfare area. This is particularly important because it allows adults to access their life histories from government agencies.[45]

25.37 The above illustrates that the differing requirements—that is, either to retain certain data or to destroy, delete or de-identify those data—depend largely on the type of information in question and the context in which it is collected.

25.38 Controversy often arises where an agency or organisation wishes to retain personal information for a longer period than is thought by some other people to be necessary. For example, some people have criticised the United States corporation that runs the search engine, Google, for having a policy of retaining for 18 months personal information that may be used to link individuals with search terms they have used in the Google search engine.[46] The company global privacy counsel, Peter Fleischer, has been cited as justifying this policy on the ground that it is necessary

> to keep information about searchers and their online explorations to protect its system against attacks; expose online scams and hackers; to improve the algorithm on which searches are based and to meet requirements by law enforcement.[47]

ALRC's view

25.39 The ALRC believes that the area of data security illustrates how it is sometimes necessary to provide differing requirements in different circumstances. As noted above, the ALRC's general position is that an individual's privacy is better protected if personal information held by an agency or organisation about the individual is

---

43 Ibid sch 1, HPP 4.2.

44 See *Archives Act 1983* (Cth).

45 See Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

46 'Google to Dump User Data after 18 Months', *Sydney Morning Herald* (online), 13 June 2007, <www.smh.com.au>.

47 Ibid.

destroyed or permanently de-identified when it is no longer needed for a permitted purpose of collection. There are, however, some situations—for example, in the areas of research and health care—where the optimum means of protecting an individual's privacy and other rights is to require an agency or organisation that holds personal information to *retain* that information for a minimum period of time.

25.40 The ALRC believes that the proposed 'Data Security' principle should continue to provide, as a general rule, that personal information held by an agency or organisation should be destroyed or permanently de-identified when no longer needed. This general rule should be able to be displaced, however, where more specific legislation applies to certain types of personal information or certain activities involving the handling of personal information.

25.41 This position reflects the view expressed by the ALRC in Chapter 15 that the proposed UPPs should set out the generally applicable requirements as to information privacy, but that it is appropriate to derogate from these general requirements in relation to particular aspects of privacy or in particular contexts.[48]

Extension of destruction and de-identification requirements to agencies

Background

25.42 As noted above, the NPPs impose a requirement to destroy or de-identify personal information in certain circumstances. This is consistent with the OECD Guidelines.[49] No equivalent obligation applies to agencies under the IPPs.

25.43 In contrast, a number of other jurisdictions impose such a requirement on government agencies. For example, Canadian government institutions must dispose of personal information in their control in accordance with the regulations and by rules promulgated by the designated minister.[50] German privacy law also requires public bodies to erase personal data in certain circumstances.[51]

25.44 Similarly, some state and territory laws require government bodies to destroy or permanently de-identify personal information when it is no longer needed.[52] For example, New South Wales government bodies must not keep personal information for any longer than is reasonably necessary for the purposes for which the information

---

48 See Proposal 15–3.

49 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), guideline 11.

50 *Privacy Act* RS 1985, c P-21 (Canada) s 6(3).

51 *Federal Data Protection Act 1990* (Germany) s 20(2).

52 See *Information Privacy Act 2000* (Vic) sch 1, IPP 4.2; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 4(2); *Information Act 2002* (NT) sch 2, IPP 4.2.

may be lawfully used, and the information must be disposed of securely and in accordance with the requirements for the retention and disposal of personal information.[53]

25.45 In IP 31, the ALRC asked whether this obligation in NPP 4.2 should be extended to agencies—that is, whether agencies should be required to destroy or permanently de-identify personal information, especially when it is no longer needed.[54]

Submissions and consultations

25.46 A very large number of stakeholders submitted that agencies should be obliged to destroy or permanently de-identify personal information when it is no longer needed. This position was supported both by government stakeholders,[55] and also non-government stakeholders.[56] The importance of destruction and de-identification was emphasised in a number of submissions. For example, one submission stated:

> The single greatest protection for personal information against unexpected and unwelcome secondary uses, and 'function creep' is to delete or de-identify it. If it no longer exists in identifiable form, it can no longer pose a risk to privacy.[57]

25.47 The Australian Government Department of Health and Ageing (DOHA) submitted that such a principle would be 'consistent with the objectives of a general set of overarching principles governing the life cycle of personal information'.[58] The OPC also noted that such a requirement already applies under some state and territory law to state and territory government bodies, and there 'appears to be no solid policy reasons why this cannot be extended to Commonwealth agencies'.[59]

25.48 Guidance was, however, sought as to when an agency or organisation no longer 'needs' to retain the personal information in question.[60] DOHA submitted that this should be defined to permit both primary and secondary uses.[61]

---

53 *Privacy and Personal Information Protection Act 1998* (NSW) s 12.

54 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–18.

55 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

56 See, eg, G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007.

57 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

58 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

59 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

60 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Confidential, *Submission PR 143,* 24 January 2007.

61 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

25.49 Other stakeholders resisted a general data destruction or de-identification principle applicable to agencies. Some stakeholders noted that the disposal obligations should depend on the context—for example, the nature of the information, why it is held, etc. The Australian Federal Police (AFP), for example, submitted that 'these obligations are best located in the legislation that regulates … particular types of personal information'. It noted that disposal obligations already apply to the AFP in a number of statutes, such as in relation to fingerprints and DNA in the *Crimes Act 1914* (Cth).[62]

25.50 The National Health and Medical Research Council (NHMRC) submitted that a general data destruction requirement would need to be subject to some exceptions in relation to health and genetic information, to take into account of the peculiar needs in those areas.[63] One solution to this problem would be to make the destruction or de-identification obligation only applicable where the agency is 'under no legal obligation to continue to retain the information'.[64]

25.51 Some stakeholders argued that the *Archives Act 1983* (Cth) already deals adequately with the destruction of records, including those containing personal information.[65] The National Archives of Australia submitted that the *Archives Act*

> is part of a cohesive management regime that ensures that records are kept for as long as they are required for business and accountability purposes, and to ensure that records of archival value are generally available to the public once they are 30 years old.[66]

25.52 It should be noted, however, that the Department of Health and Ageing seemed to see no conflict between a destruction or de-identification requirement in the privacy principles and the *Archives Act* requirements.[67]

ALRC's view

25.53 The ALRC's view is that the general requirement to destroy or permanently de-identify personal information that is no longer needed should apply both to agencies and organisations. This reform, which would represent an extension of the requirement in NPP 4.2 to include agencies, was strongly supported by a significant majority of the stakeholders that commented on this issue. There seems to be no strong policy reason to differentiate in this area between agencies and organisations, particularly given that

---

62 Australian Federal Police, *Submission PR 186,* 9 February 2007.
63 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
64 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. A similar point was made by Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.
65 Confidential, *Submission PR 165,* 1 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
66 National Archives of Australia, *Submission PR 199,* 20 February 2007.
67 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

some state and territory agencies are already subject to such provisions under state and territory law.[68]

25.54 The ALRC believes that such a reform would promote privacy protection, given that the most effective means of protecting an individual's information privacy rights is to limit access to the individual's personal information. If that information is destroyed or permanently de-identified, the information self-evidently cannot be accessed or misused.

25.55 A number of concerns were raised in relation to this reform. First, it was suggested that guidance would need to be given about when agencies and organisations no longer 'need' to retain personal information. The ALRC believes that, by adopting the substance of NPP 4.2, it will be clear that an agency or organisation would no longer 'need' the personal information, within the meaning of the data security principle, if it is no longer necessary for a purpose permitted by the proposed UPPs.

25.56 Secondly, there was concern that there may be tension between this requirement in the proposed UPPs and requirements relating to the retention or destruction of personal information in other legislation.[69] The ALRC believes, however, that differing requirements relating to destruction in the *Privacy Act* and elsewhere can be accommodated within the proposed framework. As explained above, the proposed UPPs should set out the generally applicable requirements as to information privacy, but these general requirements may be displaced by other requirements in legislation dealing with specific aspects of information handling or particular contexts.

25.57 Thirdly, as noted above, some stakeholders suggested that the destruction or de-identification obligation should only apply where the agency or organisation is under no legal obligation to retain the information. The ALRC believes, however, that such a qualification to the general principle is unnecessary because, if an agency or organisation is legally required to retain personal information, this clearly indicates that it still 'needs' it for a permitted purpose.

25.58 Finally, as noted earlier, in the proposal below and in the proposed 'Data Security' principle, the ALRC avoids using the term 'de-identify' and instead uses the term 'render non-identifiable'. This change in terminology reflects the position discussed in Chapter 3 and later in this chapter.

---

68 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW) s 12.

69 See the above submissions relating to the *Archives Act 1983* (Cth).

Proposal 25–4 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs.

When is destruction or deletion appropriate?

Background

25.59 Where an agency or organisation holds personal information about an individual, but it has no lawful reason under the *Privacy Act* or other legislation to continue to hold the information, a question arises as to what is the most appropriate course of action. There are many situations in which this may arise. For example, an agency or organisation might hold personal information about an individual that is incorrect, or it might have collected personal information without lawful authority. In such situations, should the information be deleted or otherwise destroyed? Is it more appropriate to keep some kind of record of the information but take steps to de-identify or 'mask' the information and prevent adverse consequences for the individual? Does the answer depend on the error involved and the particular information-handling context?

25.60 In IP 31, the ALRC asked whether the privacy principles should regulate the deletion of personal information—or any particular types of personal information—by organisations and agencies, or whether this is best left to OPC guidance.[70] Regulation could involve legislative prohibition or authorisation of deletion in certain circumstances.

25.61 Guidelines issued by the OPC about the IPPs provide that, where possible, an agency should generally retain old personal information, while clearly marking it as no longer current, and new information should record the date and reason the old information is superseded. The Guidelines state that:

> There may however be some particularly sensitive cases in which the mere existence of the earlier incorrect information could be detrimental. In such cases, deletion may be the only appropriate option. It is essential if information is deleted that a notation is made of the reason for the deletion and the officer responsible for the decision.[71]

---

70 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–19.

71 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998).

Submissions and consultations

25.62 A number of stakeholders were comfortable with a privacy principle that carried an obligation either to destroy or permanently de-identify personal data.[72] Such a principle, it was argued, provides flexibility in how to deal with personal information that can no longer be held lawfully by an agency or organisation. Some stakeholders stated that, while it may not always be appropriate to delete such personal information, guidance from the OPC would assist agencies and organisations in knowing how to dispose of, or otherwise deal with, such information.[73]

25.63 Some stakeholders expressed concern about the appropriateness of deleting, as distinct from annotating, incorrect records of personal information.[74] The Public Record Office of Victoria noted that, even where a record contains incorrect personal information, the best course may be to amend the record so as to leave the original incorrect data intact. This is because the incorrect data can provide 'important evidence' and may be 'of value to an individual who has a legitimate grievance against a government agency'.[75] This is not always so, however. In a case brought under the *Freedom of Information Act 1991* (SA) involving a request to amend a record containing incorrect personal information, Judge Anderson explained his decision to black out, rather than merely annotate, the relevant information:

> I recognise that the effect of this direction is to disrupt the historical integrity of the [record]. However, that is as it must be for I am unable to see that it was the intention of Parliament to preserve the historical integrity of incorrect factual assertions and any opinion based thereon.[76]

25.64 Agencies and organisations are sometimes under explicit legal obligations to retain personal information and it was feared that these obligations could conflict with a privacy principle requiring them to delete personal information in certain circumstances.[77] It was also noted that personal information often needs to be retained

---

72 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; K Pospisek, *Submission PR 104,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

73 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

74 See, eg, Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

75 Public Record Office Victoria, *Submission PR 72,* 3 January 2007. See also Government of South Australia, *Submission PR 187,* 12 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

76 *Jeffries v South Australia Police* [2003] SADC 2, [30].

77 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

because there is a chance that it will be required at a future date for, among other things, litigation purposes.[78] This can require an agency or organisation to keep the information in question for at least as long as the relevant statute of limitations.[79]

25.65 Nevertheless, it was submitted that such concerns should not permit agencies to retain personal information 'just in case'; rather, any claimed need to retain personal information 'should be addressed through specific legal requirements, which can be debated and justified as clear exceptions to a general presumption of disposal'.[80]

ALRC's view

25.66 The ALRC's view is that the OPC should provide guidance as to when it is appropriate to destroy or de-identify (in other words, render non-identifiable) personal information that is no longer needed for a purpose permitted by the UPPs. While there are undoubtedly situations where destruction of personal information would be inappropriate—for example, if the personal information may later be needed for the purposes of litigation—these situations can best be dealt with in guidance from the OPC.

25.67 As noted by a large number of stakeholders, this approach would retain a desirable level of flexibility in the proposed 'Data Security' principle. Moreover, as noted earlier in this chapter, a common sense approach to this privacy principle dictates that, where an agency or organisation is under a legal obligation to retain personal information, then this clearly indicates that it still 'needs' the information for a permitted purpose under the proposed UPPs, and so it would not be required to dispose of the information.

Proposal 25–5 The Office of the Privacy Commissioner should provide guidance about when it is appropriate for an agency or organisation to destroy or render non-identifiable personal information that is no longer needed for a purpose permitted under the UPPs. This guidance should cover, among other things:

(a) personal information that forms part of a historical record;

78 National Archives of Australia, *Submission PR 199,* 20 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Public Record Office Victoria, *Submission PR 72,* 3 January 2007.

79 AAMI, *Submission PR 147,* 29 January 2007.

80 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. See also Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

(b) personal information, or a record of personal information, that may need to be preserved, in some form, for the purpose of future dispute resolution; and

(c) the interaction between the UPPs and legislative records retention requirements.

General right to destruction of personal information?

25.68 The ALRC asked whether an individual should have the right to request an agency or organisation to destroy personal information that relates to him or her and, if so, in what circumstances or upon what conditions.[81] Any such request would have to be considered with reference to any applicable legal obligations to retain the personal information.

Submissions and consultations

25.69 A number of stakeholders opposed amending the privacy principles to give individuals the right to request agencies and organisations to destroy their personal information. Some were concerned that such a requirement would be a blunt instrument, because it would not allow agencies and organisations to deal with the information otherwise than by destruction, even if some other method would be more appropriate.[82] The Australian Bankers' Association noted, for example, that sometimes it is necessary to retain personal information 'to maintain the banking service for customer' or to enforce the customer's contractual obligations.[83] It was also suggested that, in relation to agencies delivering government services, such a provision would 'compromise … public accountability'.[84]

25.70 Moreover, some stakeholders suggested that individuals' rights of access and correction (provided in IPPs 6–7 and NPP 6) adequately address the underlying problem, without providing a right of individuals to request the destruction of their personal information.[85]

25.71 It was also suggested that such a reform could place unreasonable burdens on organisations and agencies. Some stakeholders submitted that any right to have one's

---

81 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–19.

82 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

83 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

84 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

85 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007. The right to access and correction is dealt with in Ch 12 (in relation to personal information held by agencies) and Ch 26 (in relation to personal information held by organisations).

personal information destroyed should not be located in general privacy legislation, but rather in the relevant statute that permitted the collection, use or disclosure of the information in the first place.[86] The AFP noted that this was the case for some other federal legislation, including: the *Australian Federal Police Act 1979* (Cth) and the *Crimes Act*, in relation to fingerprints, forensic material, and evidence seized on arrest or by search warrant; and the *Telecommunications (Interception & Access) Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth), in relation to intercepted communications.

25.72 Some stakeholders, though not opposed to the addition of a general right of individuals to request the destruction of personal information, submitted that such a right would need to be subject to certain qualifications. DOHA argued that the right would need to be 'subject to operational requirements', such as an agency's need to retain personal information following the provision of a service in order to consider a future application for a related service.[87] It was also suggested that the right should be subject to other statutory requirements.[88] The NHMRC submitted that the deletion of health and genetic information

> is best covered by regulations or guidelines rather than by the IPPs or NPPs, so that amendment or updating is easier if required, and difficult issues such as balancing the rights of the individual who requests deletion of their information with the rights of their genetic relatives to access the information for their own health benefit in the future can be addressed in detail.[89]

ALRC's view

25.73 The ALRC does not support giving an individual the general right to require an agency or organisation to destroy personal information it holds about the individual. None of the submissions received by the ALRC were strongly in favour of such an amendment, and a large number of submissions opposed it. This indicates that there is not a strong movement for change in this area.

25.74 Moreover, the ALRC believes that there are a number of important factors that weigh against such a change. First, the ALRC believes that such an amendment would promote undesirable rigidity in data security issues, by encouraging personal information to be destroyed even where another method of dealing with the information would be more appropriate in the circumstances.

25.75 Take the following hypothetical example. Company X, lawfully collects personal information about an individual, Y, including the details of various products

---

86 Australian Federal Police, *Submission PR 186,* 9 February 2007; Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007.

87 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

88 CSIRO, *Submission PR 176,* 6 February 2007; AXA, *Submission PR 119,* 15 January 2007.

89 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

purchased by Y. After the transaction is complete, Y may want X to remove all of Y's personal information from X's database. If the information is destroyed, however, this could make it difficult for X to analyse its sales data and liaise with product manufacturers. On the other hand, if the personal information is permanently de-identified, this may satisfy the legitimate interests of both the individual and the company, by allowing X to retain some data relating to product sales that would be useful to its business without identifying Y as the purchaser.

25.76 Secondly, it is important for the 'Data Security' principle to be sufficiently flexible to accommodate the various retention and destruction requirements that apply in other legislation to specific categories of personal information, and in particular situations. Therefore, such an amendment may hinder the ability of the *Privacy Act* to operate harmoniously with other legislation because it may conflict with other retention and destruction obligations. Archives legislation is one such example.

Meaning of 'destroy or permanently de-identify'

25.77 Assuming that an agency or organisation is subject to a requirement to destroy or permanently de-identify personal information, a related question is: how is it expected to fulfil this requirement? More specifically, should there be guidance (either in law or from the OPC) as to what an entity needs to do to destroy or permanently de-identify personal information and, if so, what should be required?

25.78 Although no specific question was directed to this issue in IP 31, a number of stakeholders considered this issue, and a number of stakeholders requested guidance in this area.

Submissions and consultations

25.79 Commenting on the IPPs, the OPC suggested that agencies should be obliged to institute 'an appropriate disposal regime … to ensure that the information is destroyed or de-identified in a secure manner'.[90] It gave the example of the disposal authority regime under the *Archives Act 1983* (Cth).

25.80 Another stakeholder suggested that destruction of data should be 'complete and non-reversible and … be readily demonstrated to be so'.[91] This is particularly important for digital records because some systems only allow for 'simple "deletion", which may keep such data on record but simply tag it as "deleted"'.[92] A similar point was made by the Commonwealth Scientific and Industrial Research Organisation (CSIRO), which noted that

> many large organisations have automated computer backup systems—and with some current backup technologies it is very difficult to remove particular files without

90 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
91 W Caelli, *Submission PR 99,* 15 January 2007.
92 Ibid.

> going through the complicated, time-consuming and risky process of restoring, deleting the files from the restored copy, re-doing the backup then destroying all the data on the original backup.[93]

25.81 According to the Victorian Society for Computers and the Law, this causes the following problem:

> [E]specially in the case of larger organisations, it may be practically impossible to guarantee the complete destruction of particular information, or if it is possible, the destruction process may be unreasonably costly and burdensome. The practical effect is that organisations requested to delete information may be encouraged to disregard such requests, to make only cursory and incomplete attempts to delete information, or to pass on the costs of deletion to consumers.[94]

25.82 The CSIRO also expressed concern about the 'confusion and lack of clarity' over the meaning of the term 'de-identification', stating:

> Sometimes it appears to mean simply that nominated identifiers such as name, address, date of birth and Medicare number have been removed from the data. At other times its use appears to imply that individuals represented in a data set cannot be identified from the data—though in turn it is completely unclear what this means. Of course simply removing nominated identifiers is often insufficient to ensure that individuals represented in a data set cannot be identified—it can be a straightforward matter to match some of the available data fields with the corresponding fields from external data sets, and thereby obtain enough information to determine individuals' names either uniquely or with a low uncertainty.[95]

25.83 The CSIRO suggested the *Health Insurance Portability and Accountability Act of 1996* (US) is 'a very good starting point' in providing guidance on the meaning of these terms.[96] It was also suggested that reference should be made in the Act to 'an accepted industry standard for secure document destruction'.[97] The Centre for Law and Genetics suggested that, following data destruction or de-identification, there should be a requirement that the entity create a record 'so that there is an audit trail that can be checked if required at some future date'.[98]

ALRC's view

25.84 The ALRC acknowledges that there is considerable confusion as to what agencies and organisations need to do in order to destroy or permanently de-identify personal information, within the meaning of the privacy principles. There is particular

---

93 CSIRO, *Submission PR 176,* 6 February 2007.
94 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.
95 CSIRO, *Submission PR 176,* 6 February 2007.
96 Ibid.
97 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.
98 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

confusion in relation to digital or electronic records of personal information, given that multiple back-up copies are often automatically made of such records.

25.85 The ALRC's view is that two steps should be taken to alleviate this confusion. First, the term 'permanently de-identify' should not be used in the UPPs, because it is at least arguable that such an obligation to 'permanently de-identify' personal information does not require taking action to preclude the possibility of re-identification at a later date.[99] The ALRC believes that any ambiguity would be removed by using the alternative term 'render non-identifiable', because this makes it clear that agencies and organisations are obliged to take steps to prevent future re-identification of data.

25.86 Take the following hypothetical example. A bank holds copies of various documents, such as the title deed, of an individual (X), who has a mortgage with the bank. After X discharged the mortgage, the bank no longer has a lawful purpose for holding these documents within the meaning of the privacy principles, and so it is required to destroy or permanently de-identify personal information contained in these documents. If the bank merely cuts out X's name wherever it appears and burns these bits of paper, arguably the documents have been permanently de-identified because it is impossible to re-insert the name at a later date. This will not necessarily preclude the documents from later being re-identified, however, if a person is able to match the data in these documents with other publicly available data, such as government land title information. On the other hand, an obligation to render the information in question non-identifiable would require the bank to take additional steps to ensure that the information in the documents cannot be easily matched with other available data to allow the documents to be re-identified.[100]

25.87 Secondly, the ALRC agrees with a number of stakeholders that further guidance should be made available as to what is required to destroy or render non-identifiable personal information. This could be provided in the *Privacy Act* itself or in guidance issued by the OPC. The problem with expanding the data security privacy principle to provide greater legislative direction is that it would undermine the objective of adopting technology neutral privacy principles that are high-level and brief.[101] Consequently, the ALRC believes that this guidance should be provided by the OPC, which can tailor its advice by taking into account the features of particular technologies that cause data security concerns. As explained in Chapter 29, this guidance should also make clear that any costs incurred in fulfilling this requirement should be treated by agencies and organisations as normal operating costs and should not be passed on to the individual concerned.

---

99 This issue is also discussed in Ch 3.
100 The issue of de-identification is considered in the specific context of research in Ch 58.
101 See Proposal 15–1.

Proposal 25–6 The Office of the Privacy Commissioner should provide guidance about what is required of an agency or organisation to destroy or render non-identifiable personal information, particularly when that information is held or stored in an electronic form.

Summary of proposed 'Data Security' principle

25.88 In summary, the ALRC's view is that the eighth principle in the proposed UPPs should be called 'Data Security'. It should appear as follows.

UPP 8. Data Security

An agency or organisation must take reasonable steps to:

(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;

(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and

(c) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

26. Access and Correction

Contents

Introduction 755
Current coverage by IPPs and NPPs 756
Scope of proposed 'Access and Correction' principle 757
Should the principle cover agencies and organisations? 757
Level of detail in the principle 758
Access by intermediaries 759
Submissions and consultations 759
ALRC's view 759
Barriers to access: fees and timeframe 761
ALRC's view 762
Right to correction of personal information 763
Background 763
Submissions and consultations 764
ALRC's view 764
Incorrect information: notification of third parties 765
Background 765
Submissions and consultations 766
ALRC's view 768
Consequential amendments 769
Notification of access rights 770
Summary of proposed 'Access and Correction' principle 771

Introduction

26.1 Australian law sets out rights and obligations in relation to individuals' access to, and correction of, personal information held by agencies and organisations. For personal information held by agencies, these rights and obligations are set out in a combination of the Information Privacy Principles (IPPs) of the *Privacy Act 1988* (Cth) and also the *Freedom of Information Act 1982* (Cth) (FOI Act). In contrast, the provisions dealing with access and correction of personal information held by organisations are set out exclusively in the National Privacy Principles (NPPs).

26.2 These provisions generally reflect the 'Individual Participation Principle' in the Organisation for Economic Co-operation and Development's *Guidelines on the*

Protection of Privacy and Transborder Flows of Personal Data (1980) (OECD Guidelines).[1] They also respond to 'a core principle' in the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995) (EU Directive)—namely, that

> the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her.[2]

26.3 This chapter concentrates on the regime for access to, and correction of, personal information held by *organisations*.[3] This chapter considers the following main questions. What should be the scope of the access and correction privacy principle? What limitations should apply to an individual's general access and correction rights? Where personal information held by an organisation is shown to be incorrect, should the organisation be required to notify any third parties to whom the information has been disclosed?

Current coverage by IPPs and NPPs

26.4 As noted above, the provisions dealing with access and correction in respect of personal information held by agencies are set out in a combination of the FOI Act and IPPs 6 and 7. IPP 6 provides that an individual is entitled to access a record containing his or her personal information, where it is in the possession or control of a record-keeper, except to the extent that the record-keeper is required or authorised to refuse access under Commonwealth law.

26.5 IPP 7 provides that a record-keeper, who has possession or control of a record containing personal information, must take reasonable steps (by way of making appropriate corrections, deletions and additions) to ensure the record is accurate and is relevant, up-to-date, complete and not misleading. Where the record-keeper is not willing to amend the record in accordance with a request by the individual concerned—and in the absence of a decision or recommendation under applicable Commonwealth law that the record should be amended—the record-keeper, if requested by the individual concerned, is to take reasonable steps to attach to the record any statement by the individual of the correction, deletion or addition sought.

---

1 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 13.

2 European Commission Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998. See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12.

3 The provisions that should apply in respect of personal information held by *agencies* are addressed in Ch 12.

26.6 For personal information held by organisations, NPP 6.1 sets out the general requirement that, if an organisation holds personal information about an individual, it must provide the individual with access to the information on request. It then lists a number of situations where access can be denied or limited.

26.7 Where an organisation is not required to provide access under NPP 6.1, the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.[4] NPP 6.2 provides that an organisation may give an individual an explanation for refusing to grant access to personal information, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.

26.8 NPP 6.5 provides that, if an individual is able to establish that personal information held by an organisation about the individual is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information. If the individual and the organisation disagree about the accuracy of the information and the individual asks the organisation to append a statement claiming the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to comply with the request.[5] Finally, NPP 6.7 provides that an organisation must provide reasons for denial of access or a refusal to correct personal information.

Scope of proposed 'Access and Correction' principle

Should the principle cover agencies and organisations?

26.9 In Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether 'the overlap of the *Privacy Act* and *Freedom of Information Act 1982* (Cth) provisions relating to access and amendment of records give rise to any difficulties'.[6] The responses by stakeholders to this question are summarised in Chapter 12. That chapter also addresses the related question whether the 'Access and Correction' principle in the proposed Unified Privacy Principles (UPPs) should cover agencies or organisations, or both?[7]

26.10 Chapter 12 sets out the ALRC's view that the rules relating to access and correction in respect of personal information held by agencies should be set out in a separate Part of the *Privacy Act*, as distinct from in the UPPs or in the FOI Act. Consequently, the ALRC believes that the proposed 'Access and Correction' principle

---

4 *Privacy Act 1988* (Cth) sch 3, NPP 6.3. Compare also s 18H, which provides that, in certain circumstances, an individual's rights of access to credit information files and credit reports may be exercised by another person authorised in writing by the individual.

5 Ibid sch 3, NPP 6.6.

6 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(a).

7 Note that the ALRC proposes to bring together the IPPs and NPPs to form the UPPs: see Proposal 15–2.

in the UPPs should deal predominantly with personal information held by organisations but, for clarity, it should also contain a note stating that the requirements on agencies in respect of access and correction are set out in the relevant Part of the *Privacy Act*.

Level of detail in the principle

26.11 NPP 6 is an example of a 'hybrid principle' in that it contains some general, high-level provisions and also some relatively prescriptive provisions.[8] It first sets out the general rule that an organisation must provide an individual with access to personal information it holds about the individual. After this, NPP 6 contains an exhaustive list of exceptions, qualifications and derogations from this general right, as well as a number of more detailed provisions that further explain the parameters of this right.

26.12 NPP 6 is, therefore, a relatively lengthy principle. The ALRC proposes that the NPPs should provide the general template in drafting and structuring the proposed UPPs,[9] which would mean that, if the structure of NPP 6 were replicated in the equivalent principle in the UPPs, the proposed 'Access and Correction' principle would remain relatively lengthy.

26.13 One option would be to move some of the detailed provisions in the proposed 'Access and Correction' principle into another part of the *Privacy Act* or into subordinate legislation. The ALRC believes, however, that the benefits of this approach would be outweighed by the disadvantages. In particular, if these provisions were moved out of the UPPs, this would require them to be re-drafted significantly so that they operate as conventional statutory provisions, as distinct from principles. Inevitably, this would make them more prescriptive and less high-level.

Proposal 26–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Access and Correction' that:

(a) sets out the requirements that apply to organisations in respect of personal information that is held by organisations; and

(b) contains a note stating that the provisions dealing with access to, and correction of, personal information held by agencies are located in a separate Part of the *Privacy Act*.

8 For discussion of the overall structure of the privacy principles, see Ch 15.
9 Proposal 15–4.

Access by intermediaries

26.14 Where an organisation has lawfully denied a request for access, NPP 6.3 requires the organisation nevertheless to consider whether it would be acceptable to provide access to a mutually agreed third party intermediary.

26.15 In 2005, the Office of the Privacy Commission (OPC) noted concern that the obligation in NPP 6.3 for an organisation merely to 'consider' the use of intermediaries, where the organisation is not required to provide access, is inadequate.[10] There is a question, therefore, whether this obligation should be strengthened.[11]

Submissions and consultations

26.16 A number of stakeholders submitted that NPP 6.3 should be amended to provide individuals with the right to have a mutually agreed intermediary access the information in question in appropriate circumstances.[12] The OPC stated that this would be more consistent with the overall intent of the principle, which is to provide individuals with the right to access their personal information.[13] It was submitted that the requirement merely to consider a request for access by an intermediary is too limited, and it was observed that there are no similar provisions in other privacy legislation.[14]

26.17 Legal Aid Queensland submitted that such an amendment may help in protecting the access rights of people with a diminished decision-making capacity.[15] The OPC also submitted that if an individual is denied access, the agency or organisation should be required to advise the individual that they may be able to gain access through the use of an intermediary.[16]

ALRC's view

26.18 Where a request for access to personal information is legitimately refused, provision for the use of a mutually agreed intermediary is important because it allows for a more flexible response. It balances the need to withhold access to personal information in appropriate circumstances with an individual's right to know what

---

10 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 114, 116.

11 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.141].

12 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

13 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

14 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

15 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

16 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

personal information is held about him or her. The objective behind this provision was explained in the explanatory material accompanying its introduction:

> [NPP 6.3] is not intended to provide a mechanism to reduce access if access would otherwise be required. There will be some cases—investigations of fraud or theft for example—where no form of access is appropriate. In other cases, it should be considered as an alternative to complete denial of access. For example, in the health context, an intermediary could usefully explain the contents of the health record to the individual as an alternative to denying access to the health information altogether.[17]

26.19 In other words, NPP 6.3 requires an organisation to consider whether a compromise can be reached that would allow an individual some form of indirect access to his or her personal information, provided that such access serves the needs of both parties. The ALRC's view is that this is a very useful provision. The question, therefore, is whether the requirement on an organisation merely to consider such a compromise provides sufficient impetus for an organisation to reach such a compromise.

26.20 The ALRC believes that it would be preferable to make some small amendments to the wording of this provision to clarify that an organisation should take reasonable steps to reach a compromise that adequately meets the needs of both parties. A requirement simply to consider such action would allow unscrupulous organisations to comply with the letter of the relevant privacy principle—by briefly contemplating and then immediately rejecting such a course of action—but ignoring the spirit of the provision, which is to allow for a more flexible approach where a blanket denial of access to personal information would be an unnecessarily blunt instrument.

26.21 The requirement to take reasonable steps should not be interpreted as requiring an organisation always to reach a compromise, or even always to try to do so. There are circumstances where a compromise, or even negotiations preliminary to such a compromise, would be inappropriate because it would undermine the organisation's legitimate reason for denying the request for access in the first place.

26.22 For example, if an individual's request for access were denied under NPP 6.1(a) on the basis that, if the individual accessed the personal information in question, it would endanger the life of a witness in criminal proceedings, it is likely to be entirely appropriate for the relevant organisation not to take any active steps to reach a compromise with the individual. Consequently, the ALRC believes that the OPC should also provide guidance as to the meaning of 'reasonable steps' in this context.

---

17 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [376]. See also Office of the Federal Privacy Commissioner, *Access and the Use of Intermediaries*, Information Sheet 5 (2001).

Proposal 26–2 (a) The proposed 'Access and Correction' principle should provide that, where an organisation is not required to provide an individual with access to his or her personal information because of an exception to the general provision granting a right of access, the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, that would allow for sufficient access to meet the needs of both parties.

(b) The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable steps' in this context, making clear, for instance, that an organisation need not take any steps where this would undermine a lawful reason for denying a request for access in the first place.

Barriers to access: fees and timeframe

26.23 The OECD Guidelines state that where an individual is entitled to access personal information about him or her, this should include the right to have it communicated:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him …[18]

26.24 These requirements have been partially incorporated in NPP 6.4, which provides that if an organisation charges for providing access to personal information, the charges must not be excessive and must not apply to lodging a request for access. Concern has been expressed that, because there is no maximum fee or schedule of fees in the *Privacy Act* for accessing personal information, a wide variety of fees may be charged. In 2005, the OPC recommended guidance be issued to the private sector regarding appropriate fee structures.[19]

18 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 13(b).

19 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 31. See also rec 29, which provides that the Australian Government should consider adopting the Australian Health Ministers' Advisory Council Code as a schedule to the *Privacy Act*, which will address the issues of intermediaries and access fees. This is discussed further in Part H.

26.25 Moreover, NPP 6 does not provide that access to personal information should be provided within a reasonable time and in a reasonable manner.[20] This contrasts with the OECD Guidelines, which contains these general provisions. Victorian privacy law sets out specifically the timeframe within which a request for access to, or correction of, personal information must be acted upon.[21]

26.26 A number of stakeholders noted that the obligations relating to fees and timeliness of service require clarification.[22] The OPC noted the difficulties in providing statutory guidance as to fees for access, and also noted that it had undertaken to provide guidance on this issue. It also stated that the privacy principle dealing with access should require agencies and organisations to provide the requested information within a 'reasonable time'.[23]

ALRC's view

26.27 The proposed 'Access and Correction' principle should require that, where an individual has a right to access personal information, the organisation should provide access within a reasonable time. Such a requirement is consistent with the OECD Guidelines, which the *Privacy Act* attempts to implement.[24] It is also consistent with the general objective behind the privacy principles to give legislative voice to information privacy rights in a way that is meaningful but not overly prescriptive.[25]

26.28 The ALRC also believes that such a requirement would not be overly onerous on organisations because it is strongly arguable that such a requirement is already implicit in NPP 6. Making this requirement explicit in the UPPs should not, therefore, require a change in practice for the vast majority of organisations that are already subject to NPP 6. For the avoidance of confusion, however, the ALRC proposes that the OPC should update its guidance relating to timeliness of service, taking account of the new explicit requirement to respond within a reasonable time.

26.29 On the other hand, the ALRC's view is that it is not desirable to provide further legislative guidance as to fees for accessing personal information. Such a provision reflects the objective that the privacy principles should be high-level and should not be overly prescriptive.[26] Moreover, it should be noted that the ALRC did not receive an indication of strong concern about the operation of this provision in submissions and consultations. The ALRC also observes that that OPC has already undertaken to

---

20 The timeframe for access is addressed in Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 49.

21 See *Information Privacy Act 2000* (Vic) sch 1, IPP 6.8 (request to be actioned no later than 45 days after receipt).

22 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

23 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

24 See the Preamble to the *Privacy Act 1988* (Cth), which is discussed in Chs 2, 4.

25 See Proposal 15–1 and accompanying text.

26 Proposal 15–1.

provide further guidance on this issue—a response that the ALRC believes is appropriate.

Proposal 26–3 The proposed 'Access and Correction' principle should provide that an organisation must respond within a reasonable time to a request from an individual for access to personal information held by the organisation. The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable time' in this context.

Right to correction of personal information

Background

26.30 A number of issues have been raised about the right to have corrected any incorrect personal information held by an organisation. The IPPs and NPPs deal with this issue differently. IPP 7 states that, in the event that there is a disagreement about correction, the record-keeper should 'attach' to the record, on request, any statement provided by the individual of the correction sought. On the other hand, NPP 6 requires the organisation, on request, to 'associate' with the information a statement that it is not accurate, complete or up-to-date.

26.31 This begs the question: which approach is more appropriate? For example, Jeremy Douglas-Stewart states:

> It may be appropriate not to attach a statement where, for example, the relevant personal information is held in electronic format in template documents that have no capacity for attachments or where the statement is very lengthy.[27]

26.32 There was also concern that the requirement in NPP 6 that an individual must establish the inaccuracy of personal information as a prerequisite to correction by the organisation is too onerous.[28] In 2005, the OPC recommended guidance on what an individual needs to do in order to establish inaccuracy.[29]

---

27 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–4810]. See also *Privacy Act 1988* (Cth) s 18J, which requires a credit reporting agency or credit provider to take reasonable steps to include in a credit file or report a statement provided by the individual of an amendment sought but not made within 30 days after being requested to do so.

28 There is no equivalent requirement under the IPPs.

29 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 32. Compare *Federal Data Protection Act 1990* (Germany) s 35(2), which contains a reverse onus of proof in that it requires a private sector body to erase certain categories of personal data where it cannot prove that they are correct.

Submissions and consultations

26.33 The Australian Privacy Foundation submitted that where the information in question is disputed, the data collector should make an annotation that is 'available to any subsequent user of the disputed information'.[30] It further submitted that the privacy principles should make clear that 'correction can take the form of amendment, deletion or addition, as appropriate in the circumstances'.[31]

26.34 The OPC submitted that the relevant provision could be amended to provide that an individual need only 'raise reasonable grounds for the organisation to believe that the information is in need of correction'.[32]

ALRC's view

26.35 Where an individual and organisation disagree as to whether the personal information held by the organisation should be corrected, the organisation is still obliged to take some action to note the individual's claim. In these circumstances, the Act provides:

> If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to *associate with the information* a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.[33]

26.36 The corresponding obligation in IPP 7.3 requires an agency to 'take such steps (if any) as are reasonable in the circumstances to *attach to any record* any statement provided by that individual of the correction, deletion or addition sought' (emphasis added). The question, therefore, is whether the obligation should be to make an attachment to the relevant record, or whether it is preferable to oblige the organisation to 'associate' with the record the views of the individual concerned.

26.37 The ALRC's view is that the wording in NPP 6.6 ('associate' rather than 'attach') is preferable because it is more technologically neutral, allowing a more flexible approach for organisations that record personal information electronically.[34] This is more likely to achieve the main objective of the relevant provision, which is to ensure that the opinion of the individual concerned is easily accessible when the organisation seeks to use or disclose the relevant personal information.

26.38 The second question noted above is whether an individual should have to establish that personal information held by the organisation is incorrect before the

---

30 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
31 Ibid. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
32 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
33 *Privacy Act 1988* (Cth) sch 3, NPP 6.6 (emphasis added).
34 Proposal 7–1.

organisation is obliged to correct the information. Only the OPC commented on this issue, recommending that this provision be amended to require the individual only to 'raise reasonable grounds for the organisation to believe that the information is in need of correction'.

26.39 The ALRC's view is that a case for amendment has not been made out. In a practical sense, clearly the individual will need to take steps to show the organisation that the relevant personal information is in need of correction. By focussing attention on the term 'establish', there is a risk that any amendment may imply that there is an onus of proof that either the individual or the organisation bears in these circumstances. This is not so. In the event of a disagreement between the organisation and individual concerned, both parties should simply be encouraged to take steps to show that the relevant information is or is not in need of correction. There is an impetus on organisations to take this approach seriously in order to comply with their obligations under the 'Data Quality' principle.

Incorrect information: notification of third parties

Background

26.40 Where an agency or organisation has corrected personal information that it holds about an individual, neither the IPPs nor NPPs oblige it to notify any third parties to whom it disclosed the inaccurate information. Similarly, the IPPs and NPPs do not require an agency or organisation to alert third parties where it has refused to make a correction pursuant to an individual's request.[35]

26.41 In its 2005 review, the OPC recommended that

> the Australian Government should consider amending NPP 6 to provide that when an individual's personal information is corrected in response to a request from the individual, the organisation should be obliged to notify third parties, where practicable, that they have received the inaccurate information.[36]

26.42 If the OPC's recommendation were adopted, it would require organisations to notify third parties of the fact that they have received incorrect information, but it would not require organisations to take the positive step of passing on corrected information to those third parties. In contrast, the United States Federal Trade Commission, in identifying core principles of data protection, has stated that 'to be meaningful, access must encompass … the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients'.[37]

---

35 This was the subject of criticism in submissions to the OPC Review: see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 116, 117.

36 Ibid, rec 28.

37 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998), 9.

Moreover, the EU Directive states that member states must guarantee that every data subject has the right to require the data controller to notify

> third parties to whom the data have been disclosed of any rectification, erasure or blocking out [that has been carried out where the data are incomplete or inaccurate] unless this proves impossible or involves a disproportionate effort.[38]

26.43 Canadian privacy law requires organisations, where appropriate, to transmit to third parties corrected personal information, or to notify those parties of an unresolved challenge concerning the accuracy of the personal information.[39] It also states that, in certain circumstances, where a government entity has disclosed personal information to third parties, it must notify them of any correction made to that information, or of any notation where the correction is not made. Where the disclosure is to a government institution, the institution must make the correction or notation on any copy of the information under its control.[40] Similarly, New South Wales privacy law provides that if personal information is amended by an agency, the individual to whom the information relates is entitled, if reasonably practicable, to have recipients of that information notified of the amendments.[41]

26.44 In Germany, public and private bodies must notify third parties of 'the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage' if this does not involve 'disproportionate effort' and 'legitimate interests of the data subject do not stand in the way'.[42]

26.45 In light of the above, the ALRC asked in IP 31:

> Should the *Privacy Act* be amended to impose an obligation on both agencies and organisations to notify third parties, where practicable, that they have received inaccurate information and to pass on any corrected information? Should an obligation to notify third parties apply where agencies or organisations have refused to make a correction?[43]

Submissions and consultations

26.46 A large number of stakeholders submitted that data collectors should be required to give appropriate notification to any third parties to whom they have disclosed personal information that has subsequently been shown to be inaccurate.[44]

---

38 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 12(c).

39 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) sch 1, Principles 4.9.5, 4.9.6.

40 *Privacy Act* RS 1985, c P-21 (Canada) s 12(2).

41 *Privacy and Personal Information Protection Act 1998* (NSW) s 15(3).

42 *Federal Data Protection Act 1990* (Germany) ss 20(8), 35(7).

43 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–25.

44 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for

26.47 Some limitations were also suggested. For example, it was submitted that the obligation should only be triggered at the request of the individual concerned.[45] The Australian Taxation Office suggested that any such obligation should not be mandatory.[46] AAMI suggested that any requirement to notify third parties should only apply where the inaccuracy is 'material',[47] which would be in line with the relevant Hong Kong provision.[48] The Law Council of Australia also noted that it would be necessary to clarify the rights and obligations of third parties that have received incorrect personal information.[49]

26.48 The OPC and others proposed a more general limitation to the requirement to notify third parties—that is, this requirement should only apply 'where reasonable and/or practicable'.[50] The OPC explained that such a limitation is important because 'requiring agencies and organisations to pass this information on as a matter of course may result in unintended consequences'. It gave the following example:

> [I]f the personal information had been collected and used by a third-party organisation for a single purpose and is no longer needed by that organisation (and therefore had been destroyed or de-identified), requiring a mandatory disclosure of the new, corrected information may result in the third-party organisation unnecessarily collecting information it had no purpose to collect or no longer needed to collect.[51]

26.49 A number of stakeholders also supported a requirement that data collectors notify third parties where they have refused to make a correction.[52] The National Health and Medical Research Council, however, saw such a requirement as unnecessary.[53]

Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

45 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

46 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

47 AAMI, *Submission PR 147,* 29 January 2007.

48 See *Personal Data (Privacy) Ordinance* (Hong Kong) DPP 2(c).

49 Law Council of Australia, *Submission PR 177,* 8 February 2007.

50 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

51 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

52 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

53 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

26.50 A smaller, but still significant, number of stakeholders argued that no general notification requirement should be introduced in these circumstances.[54] It was submitted that the case for such an amendment has not been made, nor even that this currently represents a major problem.[55] The Australian Government Department of Health and Ageing submitted that where personal information needs to be corrected 'to enable a specific service to be delivered, an obligation to do this should be set out in legislation or in contract'.[56] It was also noted that the cost of complying with such an obligation could be very onerous.[57]

ALRC's view

26.51 As a general proposition, the ALRC believes that, where an organisations has disclosed personal information to a third party, and the organisation later corrects that information in its own record, the organisation should be required to notify the third party of this correction. Such a provision was strongly supported by stakeholders and it would have a number of benefits. One obvious benefit is that it would reduce the risk that any entities to whom the incorrect personal information is disclosed will use or disclose the information inappropriately as a result of the error. Secondly, it would obviate the need for individuals to try to 'trace' where their personal information has gone in the event that it contains an error.

26.52 A number of stakeholders were concerned that such a requirement would be problematic if it were articulated in absolute terms. First, if an organisation were required to fulfil this notification obligation in every conceivable situation, it could cause enormous cost to the organisation while bringing little benefit to the individual concerned. Secondly, if the entities to which the organisation disclosed the incorrect personal information have already destroyed the personal information, it may cause more harm than it solves to disclose this personal information again.

26.53 Consequently, the ALRC's view is that any notification obligation would need to be carefully drafted in order to ensure that this obligation is neither too onerous on organisations nor likely to be counter-productive. To this end, the ALRC proposes that two important qualifications should be added to this general requirement: (1) the organisation should only be required to take 'reasonable steps' to notify any third parties; and (2) the requirement should only apply to the extent that notification would

---

54 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Confidential, *Submission PR 165,* 1 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

55 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

56 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007. See also Government of South Australia, *Submission PR 187,* 12 February 2007.

57 Queensland Government, *Submission PR 242,* 15 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

be practicable in the circumstances. These qualifications would ensure that the notification obligation is appropriately balanced and they would alleviate the concern that this new provision would lead to an unreasonable cost burden or to unintended outcomes.

Proposal 26–4 The proposed 'Access and Correction' principle should provide that where, in accordance with this principle, an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed prior to correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances.

Consequential amendments

26.54 The ALRC proposes two consequential amendments to the proposed 'Access and Correction' principle, when compared to NPP 6. First, where an individual requests an organisation to correct personal information that it holds about him or her, the individual must establish that the personal information is not 'accurate, complete and up-to-date'.[58] Although it is not stated explicitly in the explanatory material that accompanied the introduction of the NPPs in the *Privacy Act*, it seems likely that these criteria were chosen to mirror those in the Data Quality principle (NPP 3).

26.55 Consequently, there is a strong argument that the criteria in this part of the proposed 'Access and Correction' principle should be updated to reflect those in the 'Data Quality' principle in the UPPs.[59] This involves two amendments to this privacy principle: (1) adding the additional category of 'relevance'; and (2) making clear that these criteria should be interpreted with reference to a purpose of collection permitted by the UPPs.

26.56 Secondly, NPP 6.1 provides that an organisation is not required to provide access to personal information it holds about an individual to the extent that:

> (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
>
> (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual …

58 *Privacy Act 1988* (Cth) sch 3, NPP 6.5–6.6.
59 See Ch 24.

26.57 As explained in detail in Chapter 22, the ALRC believes that an exception that is triggered by a 'serious and imminent threat to the life or health of any individual' is too difficult to establish. The ALRC's view is that this exception should apply where the relevant threat is serious, but not necessarily imminent, because it would allow an organisation to take preventative action to stop a threat from developing to a point where the danger, which one is seeking to avoid, is likely to eventuate.

26.58 Consequently, the ALRC proposes to consolidate the two exceptions in NPP 6.1(a) and (b) into a single exception in the UPPs, which applies where providing access to the personal information in question would be reasonably likely to pose a serious threat to the life or health of any individual. This strikes an appropriate balance between allowing individuals to access their personal information, but preventing access where this threatens any person's life or health. Moreover, as discussed earlier in this chapter, if access is refused under this proposed exception, an individual may be entitled to gain indirect access to the information through a mutually agreed intermediary.

Proposal 26–5 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual that the individual wishes to have corrected or annotated, the individual should seek to establish that the personal information held by the organisation is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant.

Proposal 26–6 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to that information to the individual to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.

Notification of access rights

26.59 It has been noted that, unlike access to government records and the Individual Participation Principle in the OECD Guidelines, the NPPs contain no formal mechanisms to facilitate access to personal information held by organisations. Although the OPC provides guidance and information sheets on the topic,[60] it is up to each organisation to develop access procedures. In its submission to this Inquiry, the OPC stated that this discrepancy would be obviated if data collectors were required to include this in their personal information management policies.[61]

60 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001); Office of the Federal Privacy Commissioner, *Access and Correction*, Information Sheet 4 (2001).

61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

26.60 The ALRC's view is that the proposed 'Specific Notification' and 'Openness' principles will adequately cover this issue. That is, the ALRC proposes that, at or around the time of collection of personal information, agencies and organisations should be required to notify individuals that they are able to gain access to the information collected.[62] The ALRC also proposes that agencies and organisations should be required to list in their Privacy Policies the steps individuals may take to gain access to personal information about them that is held by an agency or organisation.[63] If these proposals are adopted, it would be unnecessary for the proposed 'Access and Correction' principle to include a requirement that agencies and organisations notify individuals of their rights under this principle.

Summary of proposed 'Access and Correction' principle

26.61 In summary, the ALRC's view is that the ninth principle in the proposed UPPs should be called 'Access and Correction'. It should appear as follows.

UPP 9. Access and Correction (only applicable to organisations)

9.1 If an organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:

(a) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;

(b) providing access would have an unreasonable impact upon the privacy of other individuals;

(c) the request for access is frivolous or vexatious;

(d) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(f) providing access would be unlawful;

62 Proposal 20–2.
63 Proposal 21–2.

(g) denying access is required or authorised by or under law;

(h) providing access would be likely to prejudice an investigation of possible unlawful activity;

(i) providing access would be likely to prejudice the:

(i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) protection of the public revenue; or

(iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(j) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches UPP 9.1 if it relies on UPP 9.2 to give an individual an explanation for a commercially sensitive decision in circumstances where UPP 9.2 does not apply.

9.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs UPP 9.1(a) to (j) (inclusive), the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties.

9.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

9.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, the organisation must take reasonable steps to:

(a) correct the information so that it is accurate, complete, up-to-date and relevant; and

(b) notify any other entities to whom the personal information has already been disclosed prior to correction, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.6 If the individual and the organisation disagree about whether the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete, up-to-date or relevant, the organisation must take reasonable steps to do so.

9.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

Note: If an individual wishes to access, or have corrected, personal information that is held by an agency, the individual should follow the requirements set out in the relevant Part of this Act.

27. Identifiers

Contents

Introduction 776
- Background 776
- Current coverage by IPPs and NPPs 776

Separate principle to regulate identifiers? 778
- Background 778
- Submissions and consultations 778
- ALRC's view 779

Application of 'Identifiers' principle to agencies? 779
- Background 779
- Submissions and consultations 780
- ALRC's view 781

Definition of 'identifier' 783
- Background 783
- Individual's name and ABN 783
- Biometric information 784
- Unique 785
- ALRC's view 786

Content of privacy principle dealing with identifiers 787
- Data-matching 787
- Collection of identifiers 788
- Consent to the use and disclosure of identifiers 789
- Identifiers issued by state and territory agencies 792
- Regulation of assignment of identifiers? 793

Unique multi-purpose identifiers 794
- Benefits and privacy concerns 795
- History of identification schemes in Australia 796
- The proposed access card 799
- Regulation of unique multi-purpose identifiers and the access card 803

Regulation of Tax File Numbers 805
- Background to the enhanced TFN scheme 805
- Overview of TFN regulation 806
- Fragmentation of regulation 808
- Effectiveness of current regulation 809
- ALRC's view 811

Summary of proposed 'Identifiers' principle 811

Introduction

Background

27.1 Individuals are expected or required to identify themselves in a number of different contexts. For example, information about a person's identity is often disclosed in social situations and is often required in economic transactions. The purposes of identification are manifold. For example, identification can enable interpersonal and business relationships to develop, and reduce the possibility of criminal behaviour.

27.2 The type and quantity of evidence required to establish or verify a person's identity varies according to the context in which the identification is sought. Evidence of identity can include an assertion of a person's name, the appearance or characteristics of a person, a person's knowledge (eg, a password) or the fact that a person is in possession of an object (such as a passport, birth certificate or card).[1] This chapter uses the term 'identifier' to refer to a number, symbol or other particular that uniquely identifies an individual for the purposes of an agency or organisation's operations. A more detailed discussion of the definition of 'identifier' appears below.

27.3 A number of objects that are given to individuals by organisations contain unique identifiers. Research conducted for the Office of the Privacy Commissioner (OPC) in 2004 reveals that the majority of Australians do not consider it an invasion of privacy to be asked to produce a document containing a unique identifier, such as a passport.[2] Unique identifiers may also consist of biometric information, however, such as a fingerprint or information derived from an iris scan.

27.4 This chapter examines a number of issues related to unique identifiers. It first considers whether the proposed Unified Privacy Principles (UPPs) should contain a separate principle to regulate identifiers and, if so, whether that principle should extend to the adoption, use and disclosure of identifiers by agencies. The chapter then discusses the content of the proposed 'Identifiers' principle and whether the definition of 'identifier' should be amended. The chapter also explores whether the *assignment* of identifiers should be regulated.[3] Finally, the chapter discusses the regulation of unique multi-purpose identifiers such as tax file numbers (TFNs).

Current coverage by IPPs and NPPs

27.5 The Organisation for Economic Co-operation and Development *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD

---

1 R Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7(4) *Information Technology & People* 6, 10.

2 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), [6.1].

3 The process of 'assignment' involves an entity (such as an agency) choosing an identifier to apply to an individual.

Guidelines)[4] and the Information Privacy Principles (IPPs) do not contain a principle dealing explicitly with identifiers. On the other hand, the National Privacy Principles (NPPs) currently contain a principle (NPP 7) that deals specifically with identifiers.

27.6 NPP 7 defines an identifier as including 'a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations'. An example of an Australian Government identifier is an Australian Passport number. An individual's name and Australian Business Number (ABN) are explicitly excluded from being considered identifiers for the purposes of the NPPs.

27.7 NPP 7.1 provides that an organisation must not adopt as its own identifier an identifier that has been assigned by an agency (or an agency's agent or contracted service provider).[5] Thus, NPP 7.1

> prevents an organisation from acquiring a particular government assigned identifier from all the individuals with which it deals and using that identifier to organise personal information it holds and match it with other personal information organised by reference to the same identifier.[6]

27.8 The proposed UPPs retain the distinction that is used in the NPPs between 'assigning' and 'adopting' an identifier. An entity *assigns* an identifier when the entity itself chooses an identifier that it applies to an individual. On the other hand, an entity *adopts* an identifier when it opts to refer to an individual using an identifier that has already been assigned by another entity.

27.9 NPP 7.2 provides that an organisation must not use or disclose an identifier assigned to an individual by an agency, an agency's agent or contracted service provider unless the use or disclosure:

- is necessary for the organisation to fulfil its obligations to the agency;
- falls under specified exceptions listed in NPP 2.1(e)–(h);[7] or

---

4 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

5 However, this prohibition does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances: *Privacy Act 1988* (Cth) sch 3, NPP 7.1A. See also *Privacy (Private Sector) Regulations 2001* (Cth) reg 7; *Privacy Act 1988* (Cth) s 100(2).

6 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [380].

7 NPP 2.1(ea) deals specifically with an organisation's use and disclosure of genetic information that has been collected in the course of providing a health service to an individual. In Ch 56, the ALRC proposes that provisions that relate specifically to the handling of health information should be set out in the proposed *Privacy (Health Information) Regulations*: Proposal 56–2. The proposed 'Identifiers' principle, therefore, makes it clear that, in addition to the other exceptions (which are currently listed in NPP 2.1(e)–(h)), the use and disclosure of genetic information in certain circumstances remains an exception to the prohibition against using or disclosing identifiers.

- is by a prescribed organisation of a prescribed identifier in prescribed circumstances.[8]

27.10 The final report of the OPC review of the private sector provisions of the *Privacy Act* (OPC Review) stated:

> [NPP 7] seeks to ensure that the increasing use of Australian Government identifiers does not lead to a de-facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of this data, including with other information.[9]

Separate principle to regulate identifiers?

Background

27.11 A threshold issue is whether it is necessary to retain a separate principle to regulate the use of identifiers. There is an argument that the collection, use and disclosure of identifiers could be accommodated within the privacy principles that deal with those aspects of the information cycle. For example, the proscription in NPP 7 against the adoption by an organisation of an identifier assigned by an agency could be accommodated within the privacy principle governing use of personal information.

Submissions and consultations

27.12 A small number of submissions to Issues Paper 31, *Review of Privacy* (IP 31) specifically addressed the question whether there should be a separate privacy principle to regulate the handling of identifiers.[10]

27.13 The Queensland Council for Civil Liberties supported retaining 'a clear principle prohibiting the development of a universal or approaching universal identifier.'[11] The OPC noted the current principle dealing with identifiers 'serves an important function in protecting information privacy'.

> A unique identifier can make it significantly easier to match or link personal information that has been collected in different contexts and for different purposes. Such linkages can facilitate a range of functions, such as more targeted (and potentially intrusive) direct marketing, through to data surveillance of how individuals go about their day to day lives.[12]

---

8 A number of regulations have been passed in this regard. See *Privacy (Private Sector) Regulations 2001* (Cth) regs 8, 9, 10, 11.

9 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 269.

10 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–26.

11 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

12 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

27.14 Similarly, the Northern Territory Information Commissioner was of the view that NPP 7 'currently performs a useful task in limiting the use of identifiers for data-matching and data-linkage'.[13]

27.15 Two stakeholders stated that a separate identifiers principle was not required. The Australian Government Department of Human Services submitted that a separate principle is not necessary.[14] The Insurance Council of Australia also submitted that a separate identifiers principle is not required, commenting that 'the current definition and exceptions related to identifiers are adequate'.[15]

ALRC's view

27.16 The ALRC did not receive any indication that the policy basis for the identifiers principle is no longer relevant. As discussed later in this chapter, several stakeholders were concerned that identifiers can be used to facilitate data-matching activities. Further, it has not been suggested that the dangers associated with the possible misuse of identifiers can be dealt with more effectively by incorporating the provisions relating to identifiers in other privacy principles, such as those dealing with collection, use and disclosure of personal information.

27.17 The ALRC is of the view, therefore, that the proposed UPPs should contain a separate principle that regulates identifiers. A further benefit of this approach is that the privacy principle dealing with identifiers can deal with issues unique to identifiers such as: the adoption of identifiers by agencies and organisations; the definition of the term; and the exceptions to the use and disclosure of identifiers by agencies and organisations.

Application of 'Identifiers' principle to agencies?

Background

27.18 Currently agencies are not subject to a provision regulating the adoption, use and disclosure of identifiers. In other words, the IPPs contain no provision comparable to NPP 7. In IP 31, the ALRC asked whether agencies should be subject to such a principle.[16] This question has, of course, particular pertinence in the event that the Australian Government adopts the ALRC's proposal to create a set of UPPs, applicable to both agencies and organisations.[17]

---

13 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
14 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.
15 Insurance Council of Australia, *Submission PR 110,* 15 January 2007.
16 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–28.
17 Proposal 15–2.

27.19 In contrast, some state and territory legislation regulates the assignment, adoption, use and disclosure of identifiers by public sector bodies. Under that legislation, the assignment, adoption, use and disclosure of identifiers by public sector bodies is generally prohibited unless it is necessary for the body to carry out its functions efficiently.[18]

Submissions and consultations

27.20 A number of stakeholders supported making agencies subject to a privacy principle dealing with 'identifiers'.[19] One stakeholder provided qualified support to extending the identifiers principle to agencies, provided that this does not unduly hamper longitudinal research.[20] The predominant reason given for such reform is that it would provide further protection against the misuse of identifiers—something that can breach an individual's privacy rights and increase the risk of identity theft.[21] Other reasons include that it would promote regulatory consistency between agencies and organisations.[22]

27.21 Some stakeholders submitted that it would be preferable to regulate the assignment, collection, adoption, use and disclosure of identifiers by agencies on a case-by-case basis.[23] This could be carried out either in separate sectoral legislation or in guidelines issued by the OPC. An example of such legislation is that dealing with TFNs.

27.22 Some stakeholders were opposed to agencies being subjected to an 'identifiers' principle along the lines of the current NPP 7.[24] The Australian Government Department of Health and Ageing (DOHA), for instance, stated that this would 'create significant difficulty … particularly where responsibility for delivery of services is shared between two or more agencies'. The Department gave the following example:

> While Medicare Australia delivers Medicare Services on behalf of the Australian Government, the Department of Health and Ageing has responsibility for health policy and sometimes requires individual level information for those purposes. Information provided to the Department by Medicare Australia is de-identified, with all personal demographic details removed. Each record is identified only using a personal identification number allocated by Medicare Australia. The Department would be prevented from undertaking analysis for policy purposes using that number unless some exception was included in the principle. Even though the arrangements

---

18 See *Information Privacy Act 2000* (Vic) sch 1, IPP 7.1; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7.1; *Information Act 2002* (NT) sch, IPP 7.1 (in relation to public organisations).

19 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

20 Confidential, *Submission PR 143,* 24 January 2007.

21 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

22 Ibid.

23 Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; AXA, *Submission PR 119,* 15 January 2007.

24 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

are provided for by guidelines issued under the *National Health Act 1953*, there is no exception in NPP 7.[25]

ALRC's view

27.23 The ALRC shares the view of the majority of stakeholders who responded to this question that agencies should be subject to a privacy principle dealing with identifiers. The privacy and other risks associated with the adoption, use and disclosure of identifiers by organisations also apply in respect of agencies.

27.24 Moreover, the urgency of these risks has been heightened by two modern phenomena. First, technological developments—including the prevalence of electronic record-keeping, so-called 'smartcards' and digital communication—make it increasingly difficult to maintain the security of electronic databases.[26] Secondly, as discussed earlier in this chapter, the increasing demands from government and the private sector to create new forms of identifier have increased the number of identifiers in existence. For these reasons, and given the fact that governments in Australia are intimately involved in many of these developments, the ALRC is of the view that the adoption, use and disclosure of identifiers by agencies should be regulated.

27.25 The more complex question is how the handling of identifiers by agencies should be regulated. The ALRC acknowledges, for instance, that it is very useful for agencies to be able to use identifiers already assigned by other entities in research, and in the delivery and monitoring of services. It is also recognised that differing requirements in relation to the use of identifiers may be appropriate in differing circumstances.

27.26 However, the existing NPP 7 already provides a number of exceptions to the general prohibition against using an identifier assigned by an agency (or its agent or contracted service provider). First, the combination of NPPs 7.1A and 7.2(c) creates a mechanism for the Governor-General to make regulations to prescribe an organisation that may adopt, use or disclose a prescribed identifier in prescribed circumstances, provided certain conditions are met.[27] To date, five exceptions have been made by regulation using this mechanism.[28] For instance, the regulations provide that AvSuper is a prescribed organisation for the purposes of NPP 7.1A and:

---

25 Ibid.

26 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.40], [3.43]–[3.54]; Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 114. The impact of developments in technology on privacy is discussed in detail in Part B.

27 The mechanism itself for making such an exception to the prohibition against the adoption, use or disclosure of identifiers is set out in *Privacy Act 1988* (Cth) s 100.

28 See *Privacy (Private Sector) Regulations 2001* (Cth) regs 7–11.

(b) the payroll number assigned to an individual by Airservices Australia or the Civil Aviation Safety Authority is a prescribed identifier; and

(c) the prescribed circumstance is that the payroll number is adopted by AvSuper to provide a superannuation service to the individual.[29]

27.27 In addition to the mechanism in NPP 7.1A, use or disclosure of an identifier assigned by an agency is permitted:

- where the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety;[30]

- in the case of an individual's genetic information, where the organisation reasonably believes the use or disclosure to a genetic relative of the individual is necessary to lessen or prevent a serious (but not necessarily imminent) threat to the life, health or safety of a genetic relative of the individual;

- where the organisation has reason to suspect unlawful activity, and the use or disclosure is a necessary part of its reporting or investigation of the matter;

- where it is required or authorised by law; and

- where the organisation reasonably believes that the use or disclosure is reasonably necessary for certain specified functions of an enforcement body.[31]

27.28 The ALRC's view is that these exceptions, taken together, are sufficient to allow agencies to adopt, use and disclose identifiers in appropriate circumstances. Two of these are particularly significant: the regulation-making mechanism in NPPs 7.1A and 7.2(c); and the exception that permits adoption, use or disclosure as required or authorised by law. As explained in Part C, these exceptions allow any of the federal, state and territory parliaments, or a relevant minister, to consider whether the 'Identifiers' principle should be relaxed in a particular situation and, if so, to permit this to occur. If a proposed derogation from the identifiers principle in the *Privacy Act* is particularly significant, this is likely to occur, with full parliamentary scrutiny, by the adoption or amendment of primary legislation—that is, either the *Privacy Act* or another piece of sectoral legislation. On the other hand, if the derogation is deemed to be less significant, then this can occur through the more expedited process of subordinate legislation, which still involves accountability measures, such as those provided for under the *Legislative Instruments Act 2003* (Cth). These exceptions provide sufficient flexibility to overcome any unwarranted impediments to the use of

29 Ibid reg 7.
30 See Proposal 22–3 and accompanying text.
31 *Privacy Act 1988* (Cth) sch 3, NPP 7.2(b), which imports the exceptions to the use and disclosure prohibition in NPP 2.1(e)–(h).

identifiers by agencies, while at the same time providing appropriate protection for the privacy rights of individuals.

Proposal 27–1 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Identifiers' that applies to agencies and organisations. As a consequence, s 100(2) and (3) of the *Privacy Act* should be amended to apply also to agencies.

Definition of 'identifier'

Background

27.29 The definition in NPP 7 does not describe what an identifier is, only what it includes. The definition also excludes an individual's name or Australian Business Number (ABN). The question arises, therefore, as to whether the definition of 'identifier' should be amended.

27.30 In contrast, Victorian legislation defines a 'unique identifier' as 'an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name'.[32] The OPC Guidelines to the NPPs set out a definition of 'identifier':

> A Commonwealth government identifier is a unique combination of letters and numbers, such as a Medicare number, which Commonwealth government agencies or contracted service providers allot to an individual. [33]

27.31 This section considers whether the current definition in NPP 7 should form the basis for the definition of an identifier in the 'Identifiers' principle in the proposed UPPs. The section first considers whether an individual's name and ABN should continue to be excluded expressly from the definition. The section then discusses whether the definition of 'identifier' should make clear that identifiers may comprise things other than numbers—in particular, biometric information that is not stored in an encrypted, numerical form. Finally, the section considers how to deal with identifiers that are not actually 'unique'.

Individual's name and ABN

27.32 NPP 7.3 excludes an individual's name and ABN from the definition of 'identifier'. As noted above, NPP 7 was introduced to prevent the adoption, use or disclosure of identifiers *assigned* to individuals. An individual's name is not assigned

32 See *Information Privacy Act 2000* (Vic) sch 1.
33 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 55.

by an agency or an organisation. The ALRC did not receive any submissions that suggested that the definition of 'identifier' should be amended to include an individual's name. The ALRC is of the view that, for the avoidance of doubt, an individual's name should continue to be excluded from the statutory definition of 'identifier'.

27.33 The ALRC received limited feedback about whether it remains appropriate to exclude an individual's ABN from the definition of 'identifier'. NPP 7.3 provides that an ABN has the meaning given to it in the *A New Tax System (Australian Business Number) Act 1999* (Cth). This Act provides that an

> ***ABN (Australian Business Number)*** for an entity means the entity's ABN as shown in the Australian Business Register.[34]

27.34 The Supplementary Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) explains why an ABN was expressly excluded from the definition in NPP 7:

> Although an ABN is intended to be a unique business identifier, it may, to the extent that it is assigned to identify a sole trader, also fall within the scope of the definition of *identifier* in NPP 7.3.[35]

27.35 Further, the Revised Explanatory Memorandum to the Bill states:

> The restrictions on using identifiers assigned by agencies are not intended to apply within the context of the ABN scheme. For this reason an ABN is specifically excluded from the definition of 'identifier'.[36]

27.36 NPP 7 regulates the handling of identifiers assigned to individuals—not identifiers assigned to organisations. 'Individual' is defined in the *Privacy Act* to mean a natural person.[37] An 'organisation' includes an individual who acts in a business capacity, such as a sole trader.[38] The exclusion of an ABN from the definition of 'identifier' may be a problem if there is a tendency among organisations or agencies to use the ABN of a sole trader to identify an individual acting in a non-business capacity. The ALRC, however, has not received information about such practices. For the avoidance of doubt, the ALRC is of the view that an ABN should continue to be excluded expressly from the definition of 'identifier'.

Biometric information

27.37 As discussed in Chapter 7, biometric information relates to the physiological or behavioural characteristics of a person.[39] In Chapter 3, the ALRC proposes that the

---

34 *A New Tax System (Australian Business Number) Act 1999* (Cth).
35 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 13.
36 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 147.
37 *Privacy Act 1988* (Cth) s 6(1).
38 Ibid ss 6C, 7B, 16E.
39 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

definition of 'sensitive information' should be amended to include biometric templates and biometric information collected for the purpose of inclusion in a biometric system.[40] The sensitive and permanent nature of biometric information means that it is usually advisable to store such information in an encrypted, numerical form.

27.38 The OPC, however, submitted that agencies are increasingly using unencrypted facial biometrics as identifiers.[41] For example, the Australian ePassport that was introduced in 2005 includes a digital photograph of the passport holder on a chip embedded in the centre page of the passport.[42] In addition, the Australian Government has announced that a digital photograph would be included on the surface of the proposed health benefits, veterans' and social services access card.[43]

27.39 The current definition of 'identifier' in NPP 7 does not specifically exclude biometric information. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states that identifiers are 'not limited to letters and numbers' although an identifier 'will often contain either, or both'.[44] Biometric identifiers that are not stored in an encrypted form are, therefore, probably included in the current definition. Nonetheless, for the avoidance of doubt, the OPC submitted that the wording of the definition should be amended to clarify that this is the case.[45]

27.40 The definition of personal information in Ontario privacy legislation includes 'any identifiable number, symbol or other particular assigned to the individual'.[46] The OPC suggested that the definition of 'identifier' could be based on such a broadly drafted definition.

Unique

27.41 The current definition of 'identifier' requires that it 'identify uniquely the individual for the purposes of the organisation's operations'.[47] The Office of the Victorian Privacy Commissioner submitted that some identifiers issued by agencies are not in fact 'unique'.[48] For example, Medicare numbers are listed as an example of a unique identifier in Guidelines issued by the OPC.[49] In circumstances where two or more family members share a Medicare number, however, the number does not of

---

40 Proposal 3–6.
41 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
42 A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005).
43 Australian Government Office of Access Card, *Fact Sheet—Photograph, Card Number and Signature* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/photograph-card-number-signature.pdf> at 31 July 2007.
44 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 147.
45 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
46 *Freedom of Information and Protection of Privacy Act 1990* RSO c F 31 (Ontario) s 2.1.
47 *Privacy Act 1988* (Cth) sch 3, NPP 7.3.
48 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
49 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 55.

itself uniquely identify each of those family members.[50] An amendment to the definition may be required to ensure that such numbers are in fact captured by the 'Identifiers' principle in the proposed UPPs.

27.42 Secondly, while a biometric characteristic is generally unique to an individual, it is important to note that a number of factors may affect whether a biometric system can produce an exact match between a biometric sample and a stored template. For example, the quality of a collected sample such as a facial image may be affected by lighting conditions, camera distance and lens precision. The accuracy of the match may also be affected by 'the losses introduced by the extraction of biometric features such as face geometry, and the availability of comparative biometric data from the general population'.[51]

ALRC's view

27.43 The 'Identifiers' principle was intended to cover identifiers such as the Medicare number and information other than numbers or letters. The definition of 'identifier' in the 'Identifiers' principle in the proposed UPPs should, therefore, be drafted to avoid ambiguity about the inclusion of identifiers such as the Medicare number or an individual's biometric information.

27.44 The ALRC's view is that including the words 'a symbol or any other particular' in the definition of 'identifier' would be a useful way to ensure that biometric and other non-numerical identifiers are identifiers for the purposes of the 'Identifiers' principle in the proposed UPPs. In addition, the OPC should be empowered to make a determination that, where a number, symbol or any other particular does not of itself *uniquely* identify an individual, that number, symbol or particular is still an 'identifier' for the purposes of the 'Identifiers' principle in the proposed UPPs.

27.45 This power would deal with the possible ambiguities outlined above, however such a determination would rarely be required. The proposed definition of 'identifier' would not, therefore, place a significant burden on the OPC. Further, the definition of 'identifier' notes that a determination referred to in proposed UPP 10.4(b) is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth). The inclusion of this note clarifies that any determination made by the OPC may be disallowable by the Australian Parliament.

Proposal 27–2 The proposed 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or any other particular that:

(a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or

50 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
51 M Wagner, *Correspondence*, 16 April 2007.

(b) is determined to be an identifier by the Office of the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Proposal 27–3 The proposed 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth).

Content of privacy principle dealing with identifiers

Data-matching

27.46 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifing matters of interest'.[52] The impact on privacy of data-matching is discussed in Chapter 6. In summary, privacy concerns about data-matching include: revealing previously unknown information about individuals without the knowledge or consent of those individuals; profiling of individuals; compiling data-sets without the knowledge of individuals who may then have difficulty accessing that information; accuracy of the matched data; and security of large amounts of data collected for the purposes of data-matching or data-mining.[53]

27.47 As explained in Chapter 7, data-matching is currently regulated to some extent by the principles that deal with identifiers and use and disclosure of personal information.[54] Agencies conducting data-matching programs are subject to guidelines issued by the Office of the Privacy Commissioner. In addition, the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), and binding guidelines issued under that Act, regulate the use of TFNs to match data held by certain agencies, such as the Australian Taxation Office (ATO) and Centrelink.[55]

Submissions and consultations

27.48 In IP 31, the ALRC asked whether the identifiers principle should be redrafted to deal more generally with data-matching.[56] Submissions to IP 31 indicated strong

52 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].
53 See Ch 7.
54 See the proposed 'Use and Disclosure' principle and the proposed 'Identifiers' principle.
55 Office of the Privacy Commissioner, *Data-Matching Program (Assistance and Tax) Guidelines (Annotated Version)* (1991).
56 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–26.

support for greater regulation of data-matching. A number of submissions expressed concern about the extent to which agencies and organisations could use unique identifiers to facilitate data-matching processes.[57]

27.49 Several stakeholders pointed out, however, that data-matching programs are not conducted solely by use of identifiers. For example, the Office of the Victorian Privacy Commissioner noted that data-sets may be linked through the use of names and dates of birth.[58] Similarly, CSIRO submitted that 'two databases with sufficiently many data fields in common can be matched using well-developed data linkage techniques'.[59]

ALRC's view

27.50 The ALRC is of the view that data-matching is not inherently linked to the use of identifiers. While the proposed 'Identifiers' principle provides some regulation of data-matching, in that it prohibits the adoption of an individual's identifier unless for a specified purpose, data-sets can be linked by an agency's or organisation's use of information that will not be subject to this principle. Data-matching activities of agencies and organisations should, therefore, be subject to regulation in addition to this principle. In Chapter 7, the ALRC proposes that the OPC should issue guidelines that relate to the data-matching activities of organisations.[60]

Collection of identifiers

27.51 Submissions to the OPC Review expressed concern about the collection of identifiers by organisations seeking to establish evidence of identity. For example, individuals may be asked to present a Medicare card, an Australian passport or a document with a Centrelink reference number, and such documents may be photocopied by the organisation.[61] NPP 7 does not prohibit the collection of identifiers. The OPC stated that there does not appear to be a need specifically to prohibit the collection of Australian Government identifiers because the collection of identifiers into a record is regulated by NPP 1:

> [I]f an identifier is collected by an organisation, but cannot be lawfully used or disclosed pursuant to NPP 7.2, then the collection is not necessary for one of the organisation's functions or activities. As a consequence, the collection would be prohibited by NPP 1.1.[62]

---

57 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

58 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

59 CSIRO, *Submission PR 176,* 6 February 2007.

60 Proposal 7–6.

61 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 270.

62 Ibid, 272.

Submissions and consultations

27.52 The ALRC received limited feedback on this issue. The OPC noted that it had received 'an increasing volume of enquiries regarding organisations collecting driver's licences, including the unique licence numbers'.[63] This indicates that individuals are concerned that organisations are collecting identifiers for inclusion in a record rather than merely sighting an identifier to verify the identity of an individual.

ALRC's view

27.53 The ALRC's view is that the arrangements for the collection and disposal of identifiers are adequate. Both the IPPs and NPPs currently provide that an agency or organisation should only collect personal information that is necessary for it to carry out its functions or activities.[64] This requirement will form part of the 'Collection' principle in the proposed UPPs.[65] In addition, the ALRC proposes in Chapter 18 that an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.[66] Where the collection of an identifier is not reasonably necessary for an agency or organisation to carry out its functions or activities, that collection will not be permitted and will constitute an 'interference with the privacy of an individual'.[67] The powers of the OPC to deal with interferences with privacy are discussed in Part F.

27.54 Once information has been collected for inclusion in a record, the 'Data Security' principle in the proposed UPPs provides that an agency or organisation should destroy information or render it non-identifiable if it is no longer needed for any purpose permitted by the UPPs.[68] In circumstances where an identifier is collected for a necessary purpose but it later becomes unnecessary to retain that identifier, the agency or organisation should destroy the identifier or render it non-identifiable in line with guidance issued by the OPC.[69]

Consent to the use and disclosure of identifiers

27.55 Some submissions to the OPC Review suggested that it would be beneficial to allow Australian Government identifiers to be used or disclosed in accordance with the relevant individual's consent.[70] This arguably would allow organisations to provide concessional services more efficiently. For example, an organisation may want to check with an agency to confirm that an individual is a customer of that agency and

---

63 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
64 *Privacy Act 1988* (Cth), IPP 1.1(b), NPP 1.1.
65 The 'Collection' principle in the proposed UPPs is discussed in Ch 18.
66 Proposal 18–3.
67 *Privacy Act 1988* (Cth), ss 13 and 13A.
68 Proposal 25–4. This formulation is based on NPP 4.2.
69 Proposals 25–5 and 25–6.
70 One submission to the Inquiry raised the general issue of whether an individual should be able to waive his or her right to privacy in particular cases: Confidential, *Submission PR 32,* 2 June 2006.

therefore entitled to a concession rate from the organisation. The organisation could collect an individual's Centrelink customer reference number and pass it to Centrelink to confirm the individual's eligibility for concessions. This practice, however, may be prohibited under NPP 7.[71] The OPC noted that, if this exception were allowed,

> some organisations may seek to make consent to the use and disclosure of identifiers a condition of providing a service, or a condition of providing a service at a concessional rate. The widespread collection of Australian Government identifiers may arise. This would be inconsistent with the policy intention of NPP 7, which is to ensure that Australian Government identifiers do not become de facto national identity numbers, allowing for easy aggregation of personal data across unrelated organisations.[72]

27.56 The OPC concluded that the regulation-making powers under NPP 7 and s 100 of the *Privacy Act* were sufficient. Concessional status of individuals can be checked without the risk that there will be widespread collection, use and disclosure of Australian Government identifiers.[73] The OPC recommended that the Australian Government should consider using the existing regulation-making mechanism under NPP 7 to address the issues identified in submissions regarding concessional entitlements.[74] Some states and territories provide for an exception to the use, disclosure or adoption of unique identifiers based on the individual's consent. Those jurisdictions, however, do not have comparable regulation-making powers.[75]

Submissions and consultations

27.57 Some submissions reiterated that allowing individuals to consent to the use or disclosure of their identifier in limited circumstances would assist in the provision of services to individuals. For example, the Australian Bankers' Association submitted that:

> If a bank were able to adopt and apply the Centrelink or other identifier of the customer this would facilitate identifying those customers who may wish to receive concessions on their transaction accounts.[76]

27.58 DOHA stated that organisations should be able to use an individual's identifier where the individual consents to that use and it would 'not adversely affect the individual's privacy'.[77]

---

71 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 270.
72 Ibid, 271.
73 Ibid, 272.
74 Ibid, rec 80. In this regard see *Privacy (Private Sector) Regulations 2001* (Cth) reg 9.
75 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPPs 7.2(b), 7.3(c); *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7(2)(b); *Information Act 2002* (NT) sch, IPPs 7.2(b), 7.3(b).
76 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
77 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

27.59 The OPC, on the other hand, expressed concern about the unintended effects on privacy that could result from including a broad consent exception to the identifiers principle:

> [T]he privacy risks of sharing unique identifiers are not always immediate. The risks accumulate as more organisations or agencies adopt the [identifier] for their own purposes, and as greater amounts of otherwise unrelated personal information become associated with that [identifier] … Accordingly, individuals may not always be aware of the potentially significant long term privacy risks when asked to consent to such handling, especially where they may be offered an immediate and tangible benefit or convenience.[78]

27.60 The OPC submitted that, where there is a strong public interest in an individual consenting to the handling of their identifier, such an exception should be subject to the 'process of Parliamentary scrutiny and express statement of intent for specific uses and disclosures'.[79] As discussed above, this process exists through the current exceptions to NPP 7.[80]

27.61 The Australian Government Department of Families, Community Services and Indigenous Affairs (FaCSIA) also supported a consent exception in circumstances where a person is entitled to claim concessional benefits from an organisation. FaCSIA noted that an organisation is able to confirm a person's concessional status when that person shows his or her concession card at the premises of an organisation. It is more difficult, however, for an organisation to determine an individual's concessional status when transactions occur over the telephone or internet. In particular, the inability for an individual to consent to the use of his or her Centrelink Customer Reference Number (CRN)

> is causing complications for Centrelink's Customer Confirmation eService (CCeS), which was set up to assist in the confirmation of the eligibility of customers to concessional entitlements from various state government and private sector organisations. Compelling customers to provide proof of their concession status other than through CCeS is an added burden for customers. [81]

27.62 FaCSIA submitted that the current exceptions to the identifiers principle did not adequately deal with this issue:

> The requirement for service providers to seek an amendment to the regulations is an additional and cumbersome regulatory burden. Many smaller service providers have instead opted to either deny an eligible customer of their right to a concession rate or grant a concession without undergoing a check. This is demonstrated by the fact that currently, only 33 organisations are prescribed by the *Privacy (Private Sector)*

---

78 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
79 Ibid.
80 *Privacy Act 1988* (Cth) sch 3, NPPs 7.1A, 7.2(c) and s 100.
81 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

> *Regulations 2001*, as being permitted to use Centrelink's customer reference number for the purposes of confirming an individual's concessional status.[82]

27.63 FaCSIA suggested that an alternative to an exception that would allow an individual to consent to any use of their identifier would be the inclusion of a specific exception that would allow an individual to consent to the use or disclosure of his or her CRN.[83]

ALRC's view

27.64 The ALRC notes that it would be convenient for an individual to be able to consent to the use or disclosure of his or her identifier in certain circumstances. The ALRC also notes that it may take some time and resources to develop regulations that provide for a consent exception to the prohibition on use or disclosure. On balance, however, the ALRC is of the view that a general exception that would allow individuals to consent to the use and disclosure of identifiers should not form part of the 'Identifiers' principle in the proposed UPPs as such an exception would be inconsistent with the function of the principle.[84]

27.65 Further, the current exceptions to the prohibition on use or disclosure of identifiers provide mechanisms to deal with the issues raised by stakeholders, such as the inconvenience faced by individuals seeking concessional status. Other legislation[85] or regulations issued under the *Privacy Act* can provide for circumstances where the Australian Parliament considers it appropriate for an individual to be able to consent to the use or disclosure of his or her identifier.

27.66 Prescribing specific identifiers as exceptions to the 'Identifiers' principle in the proposed UPPs does not accord with the high-level outcomes-based approach to privacy regulation that is proposed by the ALRC.[86] It is preferable for separate primary or subordinate legislation to be enacted to allow individuals to consent to the disclosure of, for example, an individual's CRN by any agency or organisation for the purpose of confirming that individual's concessional status with Centrelink.

Identifiers issued by state and territory agencies

27.67 NPP 7.1 currently prevents an organisation from adopting as its own identifier an identifer that has been assigned by an Australian Government agency; an agent of that agency acting in the capacity of an agent; or a contracted service provider of an Australian Government agent.

---

82 Ibid.
83 Ibid.
84 Consent is discussed further in Ch 16.
85 *Privacy Act 1988* (Cth) sch 3, NPP 7.2(b), NPP 2; see the proposed 'Identifiers' principle and the proposed 'Use and Disclosure' principle.
86 Proposal 15–1.

27.68 The OPC submitted that the definition of 'identifier' should be amended to include identifiers issued by state and territory agencies. The OPC noted that this would be in line with guidelines that it issued prior to the introduction of the NPPs.[87] The OPC also submitted that regulating the handling of all identifiers by organisations 'may be an appropriate response to emerging challenges posed by the risks of identity theft and fraud'.[88] Identity theft is discussed in Chapter 9.

ALRC's view

27.69 Identifers issued by state and territory agencies—for example, driver's licence numbers—do not fall within the current definition of 'identifier' in NPP 7. The ALRC is of the view that the 'Identifiers' principle in the proposed UPPs should regulate identifiers such as driver's licence numbers that are assigned by state and territory agencies and used by agencies and organisations. Such an amendment would not result in the regulation of acts and practices of state and territory agencies but rather the use by organisations and Australian Government agencies of identifiers allocated by state and territory agencies.

Proposal 27–4 The proposed 'Identifiers' principle should regulate the use by agencies and organisations of identifiers that are assigned by state and territory agencies.

Regulation of assignment of identifiers?

27.70 NPP 7 regulates the adoption, use and disclosure of identifiers by organisations. However, neither NPP 7 nor the IPPs regulate the *assignment* of identifiers by agencies or others. The process of 'assignment' involves an entity (such as an agency) choosing an identifier to apply to an individual. For example, an agency may assign an identifier, consisting of a combination of letters and numbers, to each individual to whom it provides a service. The agency would then, in its records, refer to each of those individuals by the identifier it has assigned. This should be distinguished from *adopting* an identifier, which involves an agency or organisation using an identifier that has already been assigned by another agency to refer to an individual.

27.71 Certain state and territory provisions go further than the NPPs and IPPs by regulating the assignment of identifiers—either by agencies, organisations or both.

---

87 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Office of the Privacy Commissioner, *National Principles for the Fair Handling of Personal Information* (1999); Office of the Privacy Commissioner, *Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs, Inquiry into the Privacy Amendment (Private Sector) Bill 2000*, May 2000.

88 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

There is, therefore, a gap in the federal privacy principles in that they do not regulate the assignment of identifiers.

27.72 For instance, Tasmanian and Northern Territory law both provide that certain bodies 'must not assign a unique identifier to an individual unless it is necessary for it to carry out any of its functions efficiently'.[89] Similarly, Victorian law provides that a public sector body

> must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.[90]

27.73 The ALRC received only limited feedback on whether the privacy principles should also regulate the *assignment* of identifiers by agencies. Two stakeholders said simply that they were in favour of such a reform.[91]

27.74 In relation to organisations, Electronic Frontiers Australia stated that the privacy principles

> should be amended to cover creation of unique identifiers in much the same way as collection, that is, that unique identifiers not be permitted to be created except when necessary for a particular primary purpose (eg credit card numbers), and use and disclosure be restricted to purposes directly related to the primary purpose of creation.[92]

27.75 The ALRC does not feel that it has sufficient information to make a proposal. The Commission is therefore interested in further views on this issue.

Question 27–1 Should the *Privacy Act* regulate the assignment of identifiers by agencies, organisations or both? If so, what requirements should apply and should these requirements be located in the proposed UPPs or elsewhere?

Unique multi-purpose identifiers

27.76 This section discusses unique identifiers assigned to individuals by governments for use by multiple government agencies and organisations (unique multi-purpose identifiers). The section commences by providing an overview of concerns that have been expressed about the impact on privacy of unique multi-purpose identifiers. It then

89 See *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7.1 (applicable to public and private sector organisations); *Information Act 2002* (NT) sch, IPP 7.1 (applicable to public sector organisations).

90 *Information Privacy Act 2000* (Vic) sch 1, IPP 7.1.

91 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

92 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

examines the history of identification schemes in Australia before discussing the Australian Government's proposed health benefits, veterans' and social services access card.

Benefits and privacy concerns

27.77 Schemes involving unique multi-purpose identifiers can have a number of benefits. For example, they can increase administrative efficiency and enhance data accuracy.[93] However, unique multi-purpose identifiers also raise a number of privacy concerns. One such concern is that the introduction of a unique multi-purpose identifier changes fundamentally the relationship between the individual and government.[94] In liberal democratic societies governments are accountable to their citizens. It has been argued that the introduction of a unique multi-purpose identifier symbolically reverses this tradition, making citizens accountable to their governments.[95] This could then open the way for 'further extensions of government power and … further restrictions on the individual's sphere of independent action'.[96]

27.78 It is also argued that linking a unique multi-purpose identifier to a name limits the ability of individuals to use different names in different contexts.[97] At common law, there is nothing to prevent an individual from operating under various names provided that he or she does not use different names to engage in unlawful behaviour.[98] Aliases may be used by a variety of people, such as artists and intelligence operatives.[99]

27.79 Further, the introduction of unique multi-purpose identifiers increases the ability of the state to monitor the activities of its citizens. By recording unique multi-purpose identifiers during transactions, government agencies and organisations can compile substantial amounts of information about a person, including information about a person's financial circumstances, family composition, hobbies or health. This could then be used for a variety of purposes, such as to locate a person or to determine a person's interests for the purposes of direct marketing.

---

93 See, eg, Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (1991).

94 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.7].

95 G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 163.

96 Ibid, 163.

97 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.37].

98 Ibid, Addendum, [22]. See also Ch 17.

99 R Clarke, 'Just Another Piece of Plastic for your Wallet: The "Australia Card" Scheme' (1987) 5 *Prometheus* 1, 40.

27.80 Different agencies or organisations could then combine the data collected about the transactions or activities of particular individuals to create a richer dataset. This process is known as 'data-matching'.[100] The use of a unique multi-purpose identifier facilitates greatly the data-matching process. The ability of a government to compile dossiers of personal information about individuals could have a 'chilling effect' on the activities of citizens, who no longer have a private sphere in which to relax, experiment or engage in creative pursuits.[101]

27.81 In addition, the unintended dissemination of either the identity information required to be provided by individuals in order to receive a unique multi-purpose identifier, or data generated by the use of the unique multi-purpose identifier, can erode the privacy of the individual to whom the information relates.[102] For example, such information could be stolen by a 'hacker'; accidentally disclosed through an administrative error; or deliberately sold by those with access to it, such as employees of agencies. This can increase the risk that the individual will subsequently become the victim of identity theft.[103]

27.82 Another privacy concern relates to the quality of the data involved in an identification scheme involving unique multi-purpose identifiers. Errors inputing data for the purposes of the scheme, or corruption of stored data, could adversely impact on the ability of individuals to access the services for which the unique multi-purpose identifier is required.

27.83 Finally, it has been argued that identity documents have had a long history of discriminatory uses for social control.[104] One commentator has noted that slaves in the United States were required to carry identification papers to travel, Nazis used identification cards to locate Jewish people during World War II, and the slaughter of Tutsis in Rwanda was aided by the fact that their identity cards revealed their ethnicity.[105]

History of identification schemes in Australia

Identification schemes in wartime

27.84 Several identification schemes have been implemented in wartime Australia. During World War I and World War II, all aliens (non-British subjects) were required

---

100 Ch 7 discusses in detail the practice of data-matching.

101 G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 160–161.

102 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 14.

103 Identity theft is discussed in Ch 9.

104 R Sobel, 'The Demeaning of Identity and Personhood in National Identification Systems' (2002) 15 *The Harvard Journal of Law and Technology* 319, 343. See also Privacy International, *Some Personal Views from Around the World on ID Cards* (1996) <www.privacyinternational.org> at 31 July 2007.

105 R Sobel, 'The Demeaning of Identity and Personhood in National Identification Systems' (2002) 15 *The Harvard Journal of Law and Technology* 319, 343–349.

to register with local government officials.[106] After registration, they were required to notify officials if they changed their address[107] and to produce their certificates of registration on demand.[108] In 1942, all residents of 16 years of age or above (other than aliens and other specified groups, such as members of the Defence Force performing continuous full-time war service) were required to register with local government officials in order to obtain an identity card.[109] They were then required to produce their identity cards if requested to do so by specified people, such as constables on duty.[110]

The Australia Card

27.85 In September 1985, the Australian Government announced its intention to develop a national identification scheme—the 'Australia Card' scheme[111]—to combat tax fraud, social security fraud and illegal immigration.[112] In May 1986, a Joint Select Committee on an Australia Card delivered a report that strongly recommended against the introduction of the Australia Card, suggesting a number of alternative reforms such as the computerisation of all state and territory registries of births, deaths and marriages[113] and the introduction of an upgraded, high integrity tax file number scheme.[114]

27.86 In October 1986, the Australia Card Bill 1986 (Cth) was introduced into Parliament. On two occasions the Australia Card Bill was passed by the House of Representatives[115] only to be rejected by the Senate.[116] Under s 57 of the *Australian Constitution* this became a potential trigger for a double dissolution election. Accordingly, in May 1987, the Australian Government announced Australia's sixth double dissolution election.[117] On 11 July 1987, the Australian Labor Party was returned to office and the Australia Card Bill was reintroduced into Parliament for a third time. The Bill was ultimately laid aside after Opposition senators indicated that

---

106 *War Precautions (Alien Registration) Regulations 1916* (Cth) reg 5; *Aliens Registration Act 1939* (Cth) ss 8, 13(1).

107 *War Precautions (Alien Registration) Regulations 1916* (Cth); *Aliens Registration Act 1939* (Cth) ss 9–12.

108 *War Precautions (Alien Registration) Regulations 1916* (Cth) reg 12.

109 *National Security (Man Power) Regulations 1942* (Cth) reg 32.

110 Ibid regs 45, 45A.

111 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985, 28–31.

112 R Clarke, 'Just Another Piece of Plastic for your Wallet: The "Australia Card" Scheme' (1987) 5 *Prometheus* 1, 33; Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), Addendum, [28].

113 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), rec 2(a).

114 Ibid, rec 12(a)–(d).

115 On 14 November 1986 and 25 March 1987: See R Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 31 July 2007.

116 On 10 December 1986 and 2 April 1987: See Ibid.

117 R Clarke, 'The Australia Card: Postscript' (1988) 18 *Computers & Society* 10, 10; G Greenleaf, 'Lessons from the Australia Card—Deux ex Machina?' (1988) 3(6) *Computer Law and Security Report* 6, 6.

they would disallow regulations that were required to bring crucial clauses of the Bill into effect.[118]

The Medicare card scheme

27.87 Medicare (formerly known as Medibank) commenced in 1975 to enable all eligible Australian residents to access affordable health care.[119] A unique number is allocated to most people enrolled to receive benefits under the Medicare scheme, although dependant children have the same number as one or more of their parents. On 30 June 2005, 20.5 million people were enrolled in the Medicare scheme.[120]

27.88 On 24 June 2004, the Minister for Health and Ageing, the Hon Tony Abbott MP, announced the introduction of a new Medicare smart card.[121] The card would contain the same information as a standard Medicare card, although it also had the capacity to store an optional photograph of the cardholder on the card's chip.[122] It was predicted that the card could later store patient information to facilitate patient identification in an emergency.[123] It could also later facilitate access to an electronic system of health information called Health*Connect.*[124] Some expressed concern that the card would include a Health*Connect* identification number that would be stored on the card and on the Health*Connect* database.[125]

27.89 The Medicare smart card was to be introduced on an 'opt-in' basis in Tasmania before being rolled out nationally.[126] There was limited take-up of the scheme, however, and it was terminated on 25 May 2006 in light of the Australian Government's decision to introduce the health benefits and social services access card.[127]

Other proposed identification schemes

27.90 After the bombings in London in July 2005, the Prime Minister of Australia stated that the introduction of a national identification scheme was an issue that should be 'back on the table'.[128] The introduction of such a scheme was discussed on a

---

118 G Greenleaf, 'Lessons from the Australia Card—Deux ex Machina?' (1988) 3(6) *Computer Law and Security Report* 6, 6.

119 *Health Insurance Act 1973* (Cth).

120 Medicare Australia, *About Medicare Australia* <www.medicareaustralia.gov.au> at 31 July 2007.

121 T Abbott (Minister for Health and Ageing), 'New Medicare Smartcards' (Press Release, 24 June 2004). Smart card technology is discussed in Ch 11.

122 Medicare Australia, *Medicare Smartcard* <www.medicareaustralia.gov.au/yourhealth/our_services/medicare_smartcard.shtml> at 31 July 2007.

123 Ibid.

124 Ibid. Health*Connect* and the National E-Health Transition Authority are discussed further in Ch 56.

125 R LeMay, 'Hackers on Medicare Smart Card Waiting List', *ZDNet Australia* (online), 24 February 2005, <www.zdnet.com.au/news/>.

126 T Abbott (Minister for Health and Ageing), 'New Medicare Smartcards' (Press Release, 24 June 2004).

127 Commonwealth, *Parliamentary Debates*, Senate Finance and Public Administration Legislation Committee, 25 May 2006, 126.

128 J Howard (Prime Minister), *Doorstop Interview*, 15 July 2005.

number of occasions during 2005 and early 2006.[129] On 26 April 2006, however, the Prime Minister announced that the Australian Government did not intend to proceed with the introduction of a compulsory national identity card. It did intend, however, to introduce a new card that would be required to access health and welfare benefits (the access card).[130]

The proposed access card

Overview

27.91 The Human Services (Enhanced Service Delivery) Bill 2007 (Cth) was introduced into the House of Representatives on 7 February 2007. The Bill provided a framework for the introduction of the proposed access card scheme[131] and stated that the purpose of the scheme was to improve the delivery of Commonwealth services and reduce fraud, particularly in relation to identity theft.[132] Later legislation was intended to provide detail on aspects of the scheme such as information protection, uses of the card, and review and appeal processes.[133]

27.92 On 8 February 2007, the provisions of the Bill were referred for inquiry to the Senate Finance and Public Administration Committee (the Committee).[134] The Committee released its report on 15 March 2007.[135] The Committee endorsed the 'goals to streamline the delivery of Commonwealth benefits and reduce fraud'[136] but also noted that a number of privacy concerns related to the architecture of the proposed access card scheme were not dealt with by the Bill.[137] The Committee recommended that the Bill should be combined with the proposed second tranche of legislation that was intended to provide for privacy and other individual protections.[138]

27.93 On 15 March 2007, the Minister for Human Services, Senator Chris Ellison, agreed to consolidate the first and second tranches of access card legislation.[139] At the

---

129 See, eg, C Keller, 'Identity Card Way to Prevent Rau Case: Vanstone', *The Advertiser* (Adelaide), 25 January 2006, 17; 'PM's Open Mind on ID Card', *The Australian* (Sydney), 25 January 2006, 2; M Priest, 'Ruddock to Push National Identity Card', *Australian Financial Review* (Sydney), 16 January 2006, 1.

130 J Howard (Prime Minister), P Ruddock (Attorney-General) and J Hockey (Minister for Human Services), *Joint Press Conference*, 26 April 2006.

131 Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 3.

132 Ibid cls 6, 7.

133 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 February 2007, 3 (M Brough—Minister for Families Community Services and Indigenous Affairs), 3.

134 Parliament of Australia—Senate Standing Committee on Finance and Public Administration, *Human Services (Enhanced Service Delivery) Bill 2007 [Provisions]* (2007).

135 Ibid.

136 Ibid, 11.

137 Ibid, 11.

138 Ibid, 14.

139 C Ellison (Minister for Human Services), 'Senate Committee Inquiry into Access Card' (Press Release, 15 March 2007).

time of writing in July 2007, the Australian Government is conducting consultations on an exposure draft of the consolidated legislation.[140] The following overview of the proposed access card scheme is based on information available at the time of writing.

27.94 The access card scheme is intended to enable consumers to access all health and social services with one card; access emergency relief payments through automatic teller machines and through Electronic Funds Transfer at Point of Sale (EFTPOS);[141] and reduce fraud in relation to Australian Government benefits.[142] It will also permit access card holders to use their cards for other lawful purposes.[143] The revised exposure draft Bill includes a provision stating that the access card is not to be used as a national identity card.[144]

27.95 The access card will replace up to 17 existing health care and social services cards and vouchers.[145] It will display the cardholder's name and photograph on its front, and the cardholder's signature and card number on its back.[146] Other personal information, such as the cardholder's photograph, date of birth, concession status, and details of the cardholder's children or dependants will be stored on a microchip embedded in the card.[147]

27.96 Registration for the card is intended to commence soon after the commencement of the access card legislation. The registration period will take approximately two years, after which a card will be required in order to access any health or social services benefits.[148] To register for an access card, each individual will be required to present substantial evidence of his or her identity.[149] The Australian Government has stated that the scanned images of proof of identity documents will not be stored after documents have been verified.[150] Information on the card and the chip will be stored on

---

140 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth).

141 Australian Government Office of Access Card, *Fact Sheet—Emergency Payments* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/emergency-payments.pdf> at 31 July 2007.

142 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 7.

143 Ibid cl 7(1)(e).

144 Ibid cl 7(2).

145 The health care and social services cards and vouchers that are to be replaced by the access card will include the PBS Entitlement Card, PBS Safety Net Concession Card, Pensioner Concession Card, Centrelink Health Care Card (including a Low Income Health Care Card and a Foster Child Health Care Card), Reciprocal Health Care Card, Commonwealth Seniors Health Card, Cleft Lip and Palate Card, DVA Gold, White and Orange Cards, War Widow/Widower Transport Card, Medicare Card., and other cards or vouchers prescribed by the regulations: Ibid cl 4.

146 Ibid cls 70–71.

147 Ibid cls 73–74.

148 Explanatory Memorandum Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth), 6.

149 Australian Government Office of Access Card, *Fact Sheet—Registering for an Access Card* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/registering-for-an-access-card.pdf> at 31 July 2007. The Bill allows for the making of *Administration (Identification) Rules* that will provide for the documents that are required for proof of identity: Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 184.

150 Australian Government Office of Access Card, *Fact Sheet—Registering for an Access Card* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/registering-for-an-access-card.pdf> at 31 July 2007.

a database called the Register.[151] The revised exposure draft Bill prevents the storage of certain information on the Register.[152] The Australian Government has stated that the Register will be maintained separately from existing agency databases.[153]

27.97 It is predicted that it will cost $1.09 billion over four years to establish the access card scheme and that use of the card could result in savings of between $1.6 and $3 billion dollars over 10 years.[154] The scheme will be administered by the Office of Access Card within the Australian Government Department of Human Services.[155]

The Access Card Consumer and Privacy Taskforce

27.98 On 24 May 2006, the then Minister for Human Services, the Hon Joe Hockey MP, announced the establishment of the Access Card Consumer and Privacy Taskforce (the Taskforce). The Taskforce provides independent advice to the Australian Government on a range of matters relating to the structure and operation of the Access Card scheme, including community views on the scheme and the impact of the scheme on privacy.[156]

27.99 On 15 June 2006, the Taskforce released a Discussion Paper on consumer and privacy aspects of the scheme.[157] In September 2006, the Taskforce issued a report to Government, *Issues and Recommendations in Relation to the Architecture Questions of the Access Card*.[158] In November 2006, the Minister for Human Services issued a report in response to the Taskforce's recommendations.[159] The Minister supported the majority of the Taskforce's recommendations but indicated that it would not reconsider the inclusion of a digitised signature and display of a card number on the surface of the card.[160] The Minister also disagreed with the Taskforce's recommendation that a card holder's biometric information should be stored on a card or in the Register only in the form of a template.[161] The exposure draft of the Bill that was released in December 2006 and the Bill that was introduced into Parliament in

---

151 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 35.
152 Ibid cls 36–37.
153 Australian Government Office of Access Card, *Fact Sheet—No Mega Database* (2007) <www.accesscard.gov.au/resources/pdf/factsheets/no-mega-database.pdf> at 31 July 2007.
154 KPMG, *Health and Social Services Smart Card Initiative—Volume 1: Business Case Public Extract* (2006) Prepared for the Department of Human Services, [3.5].
155 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card* (2006).
156 Ibid, 4.
157 Ibid.
158 Access Card Consumer and Privacy Taskforce, *Advice to Minister for Human Services: Report Number 1—Issues and Recommendations in relation to Architecture Questions* (2006).
159 Australian Government, *Australian Government's Response to the Access Card Consumer and Privacy Taskforce's Advice to the Minister For Human Services—Report Number 1* (2006).
160 Ibid, 8, 9.
161 Ibid, 7.

February 2007 reflected the Minister's response to the Taskforce's recommendations.[162]

27.100 On 21 February 2007, the Taskforce released a Discussion Paper on voluntary medical and emergency information that could be included on the chip contained within the access card.[163] On 13 June 2007, the Taskforce released its report on voluntary medical and emergency information, which recommended the deferral of this aspect of the access card scheme.[164] The revised exposure draft of the Bill does not include provisions relating to the inclusion on the access card of voluntary medical and emergency information.

27.101 On 23 March 2007, the Taskforce released a Discussion Paper on the registration process for the access card.[165] A report on the registration process was presented to the Minister for Human Services on 23 July 2007.[166] On 26 June 2007 the Taskforce released a report on the access card review and appeals system.[167]

The Privacy Act *and the proposed access card scheme*

27.102 The revised exposure draft Bill contains a provision stating that the access card legislation will not affect the operation of the *Privacy Act*.[168] In addition, the exposure draft Bill creates strict liability and ordinary offences for a person who adopts, uses or discloses another person's access card number unless this adoption, use or disclosure is permitted by the Bill or NPP 7, the current 'Identifiers' principle.[169] The provision of the Bill that provides exceptions to the prohibition on adopting, using or disclosing a person's access number contains a specific note stating that the section is not intended to affect the operation of NPP 7.[170]

27.103 A number of concerns have been expressed about the impact of the access card scheme on privacy. Many are the same as those discussed above in relation to unique multi-purpose identifiers generally. For example, one concern is that agencies would be able to use the access card number to link information about individuals in order to build profiles of their activities.[171] Another is that information in the Register will be targeted by those wishing to acquire large amounts of personal information for

---

162 Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth), Human Services (Enhanced Service Delivery) Bill 2007 (Cth).

163 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 2: Voluntary Medical and Emergency Information* (2007).

164 Acccess Card Consumer and Privacy Taskforce, *Report Number 2: Voluntary Medical and Emergency Information on the Access Card* (2007).

165 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 3: Registration* (2007).

166 Access Card Consumer and Privacy Taskforce, *Report Number 5: Registration* (2007).

167 Access Card Consumer and Privacy Taskforce, *Report Number 3: The Access Card Review and Appeals System* (2007).

168 Revised Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 118.

169 Ibid cl 99.

170 Ibid cl 99(4).

171 See, eg, Australian Privacy Foundation, *Why Every Australian Should Oppose the 'Access Card': The Arguments Against a National ID Card System* (2006).

some kind of gain,[172] or accessed for illegitimate purposes by government employees.[173] Others have argued that the access card will become a national identification card if it is widely used as evidence of identity in the public and private sectors.[174] Some have argued that the access card scheme is the same as the failed Australia Card scheme.[175]

27.104 Concern has also been expressed about function creep in the context of the access card scheme.[176] Currently, the *Privacy Act* allows the use or disclosure of personal information if it is required or authorised by law.[177] Accordingly, function creep will occur if legislation introduced after the implementation of the access card scheme requires or authorises new uses of personal information collected for the scheme. For example, it has been argued that photographs of cardholders collected at the time of registration could later be used to identify people on Closed Circuit Television footage.[178] Function creep will also occur if legislation introduced after the implementation of the access card scheme requires or authorises new uses for the access card, or new uses of information derived from use of the access card.[179]

27.105 It is difficult to assess concerns about the impact of the access card scheme on privacy until the architecture of the card is finalised. The ALRC intends to monitor developments relating to the scheme and expects to gain further insight into issues relating to privacy in the context of the scheme from the reports of the Access Card Consumer and Privacy Taskforce, and the finalised access card legislation (provided the legislation is finalised before the ALRC submits its Final Report).

Regulation of unique multi-purpose identifiers and the access card

27.106 In IP 31, the ALRC asked what role the *Privacy Act* should play in the regulation of unique multi-purpose identifiers.[180] An issue here is whether unique multi-purpose identifiers are different to other identifiers.

27.107 The OPC suggested that the policy intent of NPP 7, that is, to prevent identifiers from becoming de facto national identity numbers, remains relevant for Australian Government schemes such as the proposed access card.[181] Similarly,

172 See, eg, Ibid.
173 'Centrelink Scandal Highlights Smartcard Fears', *The Epoch Times* (online), 25 August 2006, <www.theepochtimes.com>.
174 The way in which the *Privacy Act* regulates the collection, use and disclosure by agencies or organisations of identifiers such as the Access Card number is discussed in Ch 4.
175 See, eg, G Greenleaf, *Quacking Like a Duck: The National ID Card Proposal (2006) Compared with the Australia Card (1986–87)* (2006) AustLII <austlii.edu.au/~graham/> at 15 June 2006.
176 See, eg, M Franklin, 'MP Warns of Access Card Misuse', *The Courier-Mail* (Brisbane), 18 July 2006, 4.
177 *Privacy Act 1988* (Cth) s 14, IPPs 10, 11; sch 3, NPP 2.
178 A Stafford, 'Access Card Could Link to Surveillance', *The Age* (Melbourne), 5 June 2006, 9.
179 *Privacy Act 1988* (Cth) s 14, IPP 10; sch 3, NPP 2.
180 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 12–3.
181 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

Graham Greenleaf, Nigel Waters and Lee Bygrave of the Cyberspace Law and Policy Centre submitted that:

> The privacy principles in the Privacy Act, and methods for adjudication concerning breaches of them, should apply to any unique multi-purpose identifiers adopted in Australia. Any variations from the application of any of the principles should be defined by specific legislative provisions stating exceptions or variations, and not left to inference from the existence of a different set of principles. Such an approach will (i) ensure that variations are obvious; (ii) facilitate a consistent body of law emerging on both the core principles and the exceptions.[182]

27.108 The Australian Government Department of Human Services submitted that access card numbers would not be 'unique' as a number displayed on the surface of an access card would be re-issued each time that the card was re-issued.[183]

ALRC's view

27.109 The ALRC's view is that the proposed access card number is likely to fall within the definition of 'identifier' in the 'Identifiers' principle in the proposed UPPs. 'Unique' does not carry with it a requirement of permanence. The proposed 'Identifiers' principle requires only that an identifer uniquely identify the individual for the purposes of that agency's or organisation's operations.[184] It has not been suggested that the proposed access card numbers will identify more than one individual.

27.110 The 'Identifiers' principle in the proposed UPPs is intended to continue to regulate aspects of information handling that are not covered by specific legislative regimes establishing unique multi-purpose identifiers. Any exceptions to the 'Identifiers' principle in the proposed UPPs should be clearly set out in legislation establishing such schemes.

27.111 The ALRC also proposes that the OPC should be empowered to direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment that relates to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information. Further, the Privacy Commissioner should have the power to report to the relevant minister an agency or organisation's failure to comply with such a direction.[185] As discussed above, unique multi-purpose identifiers present significant privacy concerns. The ALRC proposes that any Australian Government agency that intends to introduce such an identifier should notify the OPC of this intention early in the process and, in conjunction with the OPC, consider the need for a privacy impact assessment.

---

182 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

183 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

184 Proposal 27–2.

185 Proposal 44–4.

Proposal 27–5 Before the introduction by agencies of any unique multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment.

Regulation of Tax File Numbers

Background to the enhanced TFN scheme

27.112 In May 1988, following the demise of the Australia Card scheme, the Treasurer, the Hon Paul Keating MP, announced that the Australian Government intended to introduce an enhanced TFN scheme.[186] In 1988, legislation establishing such a scheme was passed.[187]

27.113 Before 1988, TFNs were simply numbers used by the ATO to match taxpayers' returns to the ATO's computer records.[188] No evidence of identity was required before a TFN was allocated to a taxpayer and there was no widespread use of TFNs by employers or employees.[189]

27.114 The enhanced TFN scheme was designed to reduce tax evasion by improving the ATO's ability to match information received from certain sources, such as financial institutions and employers, to individual tax returns.[190] Under the scheme, any person could apply to the Commissioner of Taxation for a TFN.[191] If satisfied of an applicant's identity, the Commissioner would provide the applicant with a unique TFN,[192] which could then be quoted when the applicant commenced employment or engaged in certain investment activities.

27.115 At the time the TFN scheme was introduced there were concerns that it would become a 'de facto national identification scheme',[193] and the legislation introducing the scheme contained provisions to safeguard against this. For example, it contained a provision making it an offence to require or request a TFN (including the

186 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985.
187 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).
188 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [4.8].
189 Ibid, [4.8].
190 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 September 1988, 858 (P Keating—Treasurer).
191 *Income Tax Assessment Act 1936* (Cth) s 202B.
192 Ibid s 202BA.
193 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Feasibility of a National ID Scheme; The Tax File Number* (1988), Ch 10.

TFN of entities other than natural persons) in unauthorised circumstances.[194] In addition, the *Privacy Act*, which was passed around the same time as the legislation introducing the enhanced TFN scheme, contained provisions designed to protect the privacy of individuals under the new TFN scheme.

27.116 The TFN scheme has been expanded since it was introduced in 1988. For example, since 1991 individuals have been required to provide their TFNs in order to obtain any federal income support.[195] Centrelink is permitted to use TFNs to match records between the ATO and specified assistance agencies,[196] such as Centrelink and the Australian Government Department of Veterans' Affairs,[197] in order to 'detect where a person has provided inconsistent information to one or more agencies and is thereby receiving incorrect payments'.[198]

27.117 The TFN scheme provides an example of 'function creep' in the context of unique multi-purpose identifiers. Function creep occurs when personal information or a system is used in a manner that was unintended at the time the information was collected or the system devised.[199] One commentator has stated that function creep in the TFN scheme demonstrates 'how privacy promises made in law can be lost over a very short period of time'.[200]

Overview of TFN regulation

Legislation

27.118 The handling of TFNs is regulated under various federal Acts. For example, Part VA of the *Income Tax Assessment Act 1936* (Cth) includes provisions allowing the Commissioner of Taxation to supply correct TFNs to financial institutions if a person has quoted an incorrect TFN. The *Taxation Administration Act 1953* (Cth) prohibits requirements that TFNs are to be quoted or recorded.[201] Other pieces of legislation regulating TFNs include the *Superannuation Industry (Supervision) Act 1993* (Cth), *Income Tax (Deferred Interest Securities) (Tax File Number Withholding Tax) Act 1991* (Cth), and the *Social Security Act 1991* (Cth).[202]

---

194 *Taxation Administration Act 1953* (Cth) s 8WA. Section 8WB of the *Taxation Administration Act 1953* (Cth) makes it an offence to record, use or disclose a person's TFN in unauthorised circumstances.

195 Office of the Federal Privacy Commissioner, *Submission to the House of Representatives Standing Committee on Economics, Finance and Public Administration Review of the ANAO Audit Report No. 37 1998–99 on the Management of Tax File Numbers*, 1 November 1999, Attachment E.

196 *Data-matching Program (Assistance and Tax) Act 1990* (Cth).

197 Ibid s 3.

198 Commonwealth, *Parliamentary Debates*, House of Representatives, 20 December 1990, 4871 (G Bilney—Minister for Defence Science and Personnel).

199 Office of the Privacy Commissioner, *An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*, Consultation Draft (2004), [3].

200 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 13.

201 Subject to exceptions: *Taxation Administration Act 1953* (Cth) pt III div 2 subdiv BA.

202 The regulation of TFNs is also discussed in Ch 12.

27.119 The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) (*Data-matching Act*) regulates data-matching using TFNs. Data-matching involves bringing together data from different sources and comparing them. Much of the data-matching done by Australian Government agencies subject to the *Privacy Act* is to identify people for further action or investigation for overpayment or fraud.[203]

27.120 The *Data-matching Act* sets out a number of steps in a data-matching cycle including a time frame for completing data-matching, the purposes for which matched data can be used, and the destruction of data collected.[204] Section 12 of the Act requires the Privacy Commissioner to issue guidelines for the conduct of the data-matching program.

Data-matching guidelines

27.121 The *Data-matching Program (Assistance and Tax) Guidelines* came into effect in April 1997.[205] A breach of the Act or guidelines constitutes an interference with privacy under s 13 of the *Privacy Act*, and a person may complain to the Privacy Commissioner if he or she considers a breach may have occurred.[206] In the event of a complaint being made it is dealt with in accordance with the provisions of Part V of the *Privacy Act*.[207]

Tax File Number Guidelines

27.122 Section 17 of the *Privacy Act* enables the Privacy Commissioner to issue legally binding guidelines concerning the collection, storage, use and security of 'tax file number information'.[208] 'Tax file number information' is defined as 'information … that records the tax file number of a person in a manner connecting it with the person's identity'.[209] The Privacy Commissioner's guidelines are binding on all 'file number recipients'[210]—namely, people who are 'in possession or control of a record that contains tax file number information'.[211]

---

203 Office of the Privacy Commissioner, *Data-Matching* <www.privacy.gov.au/act/datamatching> at 31 July 2007.

204 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) pt 2.

205 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997). These Guidelines replaced the Guidelines originally set down in sch 2 to the *Privacy Act 1988* (Cth).

206 *Privacy Act 1988* (Cth) s 14.

207 Ibid s 14. Legislation and guidelines that regulate data-matching activities that do not include TFNs are discussed in Ch 7.

208 Interim guidelines set out in sch 2 of the *Privacy Act* applied until the Privacy Commissioner's guidelines issued under s 17 took effect: Ibid s 17(4).

209 Ibid s 6.

210 Ibid s 18.

211 Ibid s 11.

27.123 The Privacy Commissioner issued TFN guidelines in 1992.[212] These Guidelines provide that the TFN scheme is not to be used as a national identification scheme.[213] In no situation is it mandatory for an individual to disclose his or her TFN, although non-disclosure in certain situations may have adverse financial consequences. For example, if an individual chooses not to quote his or her TFN when commencing employment, he or she will be taxed at the maximum applicable tax rate.[214] TFNs can only be collected by certain persons and organisations[215] and must not be used to establish or confirm an individual's identity for a purpose not authorised by taxation, assistance agency or superannuation law.[216] In addition, TFNs are not to be used to match personal information about an individual except as authorised by taxation, assistance agency or superannuation law.[217]

27.124 The Guidelines also require file number recipients to take all reasonable steps to ensure that security safeguards and procedures are in place to prevent unauthorised access to, or modification, disclosure or loss of, TFN information.[218] Further, file number recipients may dispose of TFN information if it is no longer required for legal or administrative purposes.[219]

Fragmentation of regulation

27.125 In IP 31, the ALRC asked whether federal legislation relating to the handling of TFNs and data-matching should be consolidated in the *Privacy Act*.[220]

27.126 The OPC submitted that:

> As the Privacy Act focuses on the personal information of individuals, it would not seem a comfortable fit to import provisions that deal with corporations and entities … In absence of a clearly identified failure in the law, the Office sees no compelling reason to move the criminal offence provisions of the *Taxation Administration Act 1953* to the Privacy Act.
>
> In regard to data-matching provisions, the Office has no strong views on the merits of incorporating the protections of the *Data-matching Program (Assistance and Tax) Act 1990* into the Privacy Act.[221]

27.127 The Australian Privacy Foundation was of the view that

---

212 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
213 Ibid, 1.1.
214 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 12.
215 The Privacy Commissioner and the former Insurance and Superannuation Commissioner (now the Australian Prudential Regulations Authority (APRA)), have complied a list of 'Classes of Lawful Tax File Number Recipients': see Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
216 Ibid, [2.1], [5.1].
217 Ibid, [2.3].
218 Ibid, [6.1].
219 Ibid, [6.2].
220 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 7–6(g).
221 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

> The use of tax file numbers should be addressed partly in tax law and partly in revised provisions of the Privacy Act dealing generically with government identifiers …
>
> The specific Data-matching legislation seems to be well established and compliance does not seem to be a problem. There seems no reason to change this law, other than as one way of extending the scope …

27.128 It appears that the current arrangements are working satisfactorily. The ALRC's view is that there no compelling reason to consolidate the federal legislation relating to the handling of TFNs and data-matching of TFNs.

Effectiveness of current regulation

27.129 In IP 31, the ALRC asked whether the schemes that regulate TFNs remain appropriate and effective.[222]

27.130 The ATO stated that 'TFNs are effectively protected; indeed, according to the Issues Paper, less than 5% of the complaints received by the Privacy Commissioner in 2004–05 related to TFNs'.[223]

27.131 The OPC submitted that the *TFN Guidelines*[224] and criminal provisions dealing with unauthorised use and disclosure[225] result in 'an effective dual-layered privacy framework'. The OPC also suggested that it may be appropriate to conduct a review of the *TFN Guidelines*.

> Such a review would provide an opportunity to consult with stakeholders on matters where the Guidelines may be able to be improved. It would also be consistent with established good regulatory practice, which holds that regulatory instruments be reviewed at intervals of no more than 10 years.[226]

27.132 The Australian Privacy Foundation also favoured a review of the *TFN Guidelines*, noting the 'function creep' that has occurred since the introduction of the enhanced TFN scheme, along with 'subsequent developments in datamatching and identity management'.[227]

Treasury review

27.133 Reform to the regulation of taxpayer information, including TFNs, is the subject of a current Australian Government Treasury review into secrecy and

---

222 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 12–2.
223 Australian Taxation Office, *Submission PR 168,* 15 February 2007.
224 *Privacy Act 1988* (Cth) s 17.
225 *Taxation Administration Act 1953* (Cth) s 8.
226 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
227 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

disclosure provisions in Australian taxation law.[228] In a Discussion Paper released in September 2006, the Treasury suggested that a standard definition of 'protected information' could be adopted in the taxation laws that deal with secrecy and disclosure of tax information.[229] This definition of 'protected information' may include TFNs in addition to details provided to the ATO on tax return forms and Business Activity Statements.[230]

27.134 The Treasury Discussion Paper also considers whether an individual should be allowed to consent to the disclosure to third parties of taxpayer information (which may include TFNs) by the ATO in some circumstances.[231] Further, the Discussion Paper canvasses whether additional disclosure of taxpayer information should be permitted for law enforcement purposes.[232]

Regulatory burden

27.135 A review of the *TFN Guidelines* could consider the regulatory burden imposed by current TFN regulation. The ATO submitted that if the ALRC found that the use of TFNs imposed a regulatory burden on businesses, the ATO could 'be involved in discussions to address this issue'. [233]

27.136 The ALRC received few submissions that addressed compliance burden in relation to TFNs. With respect to the disclosure of TFNs, Link Market Service noted that, in some circumstances, prohibiting a shareholder from providing consent to disclosure of their TFN can be time-consuming and resource intensive.

> When there are certain capital events in the life of a company, where the company's register is merged with another company's register or split into different registers TFNs cannot normally pass across to the new register. A registry provider such as Link will, on behalf of the company, send out TFN forms for shareholders to complete … This process takes time from the registry and shareholder perspective and costs the company, initiating the mail out, cost. When the registers merge or split there is no automatic transference of details and the whole exercise must be repeated. This can lead to shareholder complaints, specifically where the TFN form is not completed after the merge or split and the shareholder's dividend is subject to withholding tax as a result.[234]

27.137 The Mortgage and Finance Association of Australia noted that requirements to delete or physically remove TFNs from documents are 'costly, prone to error,

---

228 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006).
229 See, eg, *Taxation Administration Act 1953* (Cth).
230 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006), 10.
231 Ibid, 27.
232 Ibid, 29.
233 Australian Taxation Office, *Submission PR 168,* 15 February 2007.
234 Link Market Service, *Submission PR 2,* 24 February 2006.

inconvenient and unnecessary'. The Mortgage and Finance Association stated this is particularly so given that collection, use and disclosure of TFNs is strictly regulated.[235]

27.138 Any consideration of compliance burden in a review of the *TFN Guidelines* must be balanced against the reasons behind the privacy protections afforded to TFNs. The OPC noted that such protections were introduced

> to ensure that such numbers do not become de facto unique identifiers for use by all government agencies and the private sector … this remains relevant and appropriate, particularly given the increased ability of information technology to link records of information across disparate sources.[236]

ALRC's view

27.139 The ALRC is of the view that the *TFN Guidelines* should be subject to a review by the OPC, in consultation with the ATO and other relevant stakeholders. The review could consider: the policy intention behind the privacy protection of TFNs; the compliance burden that arises from TFN regulation; the Treasury review into secrecy and disclosure provisions in taxation law; and any relevant legislation that arises from the Treasury review.

27.140 Further, as discussed in Chapter 44, the *TFN Guidelines* should be renamed the *TFN Rules* to reflect that the guidelines are binding and that a breach constitutes an interference with privacy under s 13 of the *Privacy Act.*[237]

Proposal 27–6 The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the *Tax File Number Guidelines* issued under s 17 of the *Privacy Act.*

Summary of proposed 'Identifiers' principle

27.141 In summary, the ALRC's view is that the tenth principle in the proposed UPPs should be called 'Identifiers'. It should appear as follows.

UPP 10. Identifiers

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

235 Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007.
236 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
237 *Privacy Act 1988* (Cth) s 13(b). See Proposal 44–2.

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.2 An agency must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) another agency;

(b) an agent of another agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.3 The requirements in NPPs 10.1 and 10.2 do not apply to the adoption by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2), as proposed to be amended.

10.4 Where an identifier has been 'assigned' within the meaning of UPP 10.1 or 10.2, an agency or organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the agency or organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure;

(c) the identifier is genetic information and the use or disclosure would be permitted by the proposed *Privacy (Health Information) Regulations*; or

(d) the use or disclosure is by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

10.5 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or any other particular that:

(a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or

(b) is determined to be an identifier by the Office of the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999*, is not an 'identifier'.

Note: A determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* (Cth).

28. Transborder Data Flows

Contents

Introduction 815
Extra-territorial operation of the *Privacy Act* 817
National Privacy Principle 9 821
- Application of the 'Transborder Data Flows' principle to agencies 822
- Definition of 'transfer' 826
- 'Someone' in a 'foreign country' 827
- 'Reasonably believes' 828
- Reasonable expectations of the individual 829
- Interests and benefit of the individual 830
- 'Reasonable steps' 830
- Accountability 832
- Interaction with the 'Use and Disclosure' principle 835

Related bodies corporate 836
The role of the Privacy Commissioner 838
Requirement of notice that personal information is being sent overseas 844
International privacy protection 848
- European Union Data Protection Directive 848
- Asia-Pacific Economic Cooperation Privacy Framework 854
- Asia-Pacific Privacy Charter Initiative 858
- Trustmarks 861

Summary of proposed 'Transborder Data Flows' principle 862

Introduction

28.1 'Transborder data flow' refers to the movement of personal information (or data) across national borders.[1] While the focus of the *Privacy Act 1988* (Cth) was originally on personal information collected and handled within Australia, the increasing ease with which information can be transferred between countries has forced jurisdictions to recognise that efforts to protect personal information should be harmonised.[2]

---

1 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 1.

2 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), vii.

> Modern business is increasingly borderless. The communications revolution and the reduction in international trade barriers has allowed business to globalise and for regions to specialise. The call centre answers the phone in India, the product is designed in Europe, made in China and it is all managed from the US. But these business units must share their information; information about employees, customers and suppliers.[3]

28.2 Overseas business processing centres are increasingly handling customer data in such sensitive areas as processing credit card applications and bills, mortgage applications, insurance claims and help desk services.[4] It is important for Australians to feel confident that if their personal information is transferred outside Australia, it will be protected to the same standard that they enjoy in Australia. A number of respondents to the ALRC's National Privacy Phone-In expressed concerns about Australian companies sending their personal information offshore, particularly to overseas call centres.

> If I deal with a company in Australia, I most certainly do not want that company passing my details overseas, where laws about privacy are even weaker. I also have a right to know when paying online whether my payment details are being sent overseas, as I view this as a huge security risk.[5]

28.3 Economic development is dependent on globalisation of information and electronic commerce. In the 1970s and 1980s, international bodies developed the first instruments to harmonise laws within economic communities and improve trade relationships. The 1980 Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (OECD Guidelines) was one of the first international instruments that attempted to address this issue.

28.4 The OECD Guidelines provide that, in developing laws and policies to protect privacy and individual liberties, member countries should not enact laws that unnecessarily create obstacles to transborder flows of personal data.[6] The privacy principles in the OECD Guidelines are the foundation for the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) set out in the *Privacy Act*. NPP 9 governs transborder data flow out of Australia.[7]

---

3 K Sainty and A Ailwood, 'Implications of Transborder Data Flow for Global Business' (2004–2005) 1 *Privacy Law Bulletin* 101, 101.

4 B Cruchfield George and D Roach Gaut, 'Offshore Outsoucing to India by EU and US Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing' (2006) 6 *Universtiy of California Business Law Journal* 13, 13.

5 *National Privacy Phone-In* June 2006, Comment No 433. On 1 and 2 June 2006, the ALRC invited members of the public to telephone the office to provide their views and experiences of privacy protection in Australia. In total, the ALRC received 1,343 responses by telephone and via the website.

6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 18.

7 The IPPs and OECD Guidelines do not contain a comparable transborder data principle to NPP 9. The transfer of personal information outside Australia by agencies is discussed below.

28.5 More recent examples of these instruments are the privacy principles adopted by the European Union (EU) under the 1995 European Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[8] (EU Directive) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[9] The Asia-Pacific Privacy Charter Council, a regional non-government expert group, has also done work on developing independent privacy standards for privacy protection in the Asia-Pacific region.[10] Australia's ability to meet the expectations of privacy protection demanded by the international community is important to ensure that Australian businesses are not disadvantaged in an international market.

28.6 This chapter first looks at regulation of transborder data flow under the *Privacy Act* via the extra-territorial operation of the Act, and the restrictions in NPP 9 on the transfer of personal information to countries with differing privacy regimes. It considers the adequacy of the protection offered under NPP 9, including whether the principle should be expanded to apply to agencies, and the difficulties that may be experienced by businesses in complying with its requirements. The chapter then considers the adequacy of the *Privacy Act* in the context of the EU Directive, the APEC Privacy Framework and the Asia-Pacific Privacy Charter.

Extra-territorial operation of the *Privacy Act*

28.7 Section 5B of the *Privacy Act* applies the Act (and approved privacy codes) to acts done, or practices engaged in, outside Australia by an organisation, if the act or practice relates to personal information about an Australian citizen or permanent resident and either the organisation:

- is linked to Australia by being a citizen; or a permanent resident; or an unincorporated association, trust, partnership or body corporate formed in Australia; or

- carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.

28.8 Section 5B(4) extends the enforcement powers of the Privacy Commissioner to overseas complaints that fall within the criteria in s 5B(1).[11] The purpose of s 5B is to stop organisations avoiding their obligations under the Act by transferring the handling of personal information to countries with lower privacy protection standards.[12] The

---

8 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

9 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

10 See G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007. These instruments are discussed later in the chapter.

11 The enforcement powers of the Privacy Commissioner are considered in Ch 46.

12 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [1-460].

privacy laws of another country, however, will not be overridden by the *Privacy Act*. Where an act or practice is required by an applicable law of a foreign country, it will not be considered a breach of the *Privacy Act*.[13]

Agencies

28.9 Section 5B applies to organisations, but not to agencies. It is unclear whether, in the absence of an express statement, the *Privacy Act* operates extraterritorially in relation to the acts and practices of agencies. It could be argued that the IPPs apply to the records of Australian Government agencies wherever they might be.

28.10 The High Court has held, however, that in the absence of unambiguous language to the contrary, there is a common law presumption that courts do not read extra-territorial jurisdiction into legislation.[14] This presumption has been held to apply in the case of legislation that applies to agencies.[15] There are a number of examples of federal legislation that regulates the Australian Government public sector and expressly provides that the legislation is to have extraterritorial application.[16]

28.11 In the ALRC's view, agencies that operate outside Australia should be subject to the *Privacy Act*. Agencies often compel the collection of personal information and should therefore remain accountable for the handling of that information under the *Privacy Act*, whether they are located in Australia or offshore. Further, agencies should not be able to avoid their obligations under the Act by transferring the handling of personal information to entities operating in countries with lower privacy protection standards. The ALRC proposes that the *Privacy Act* be amended to clarify that it applies to the acts and practices of agencies that operate outside Australia.

Proposal 28–1 The *Privacy Act* should be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.

Information held under the law of a foreign country

28.12 The *Privacy Act* provides that where overseas acts and practices are required by an applicable foreign law, they are generally not considered interferences with the

---

13 *Privacy Act 1988* (Cth) s 13D.

14 *Jumbunna Coal Mine NL v Victorian Coal Miners Association* (1908) 6 CLR 309.

15 In *Brannigan v Commonwealth*, the appellant worked for the Australian High Commission in London. She complained of breaches of the *Racial Discrimination Act 1975* (Cth), *Sex Discrimination Act 1984* (Cth) and the *Disability Discrimination Act 1992* (Cth) while she was working at the High Commission. The Federal Court of Australia held that it lacked jurisdiction to determine the matter because the Acts did not state expressly that they operated extraterritorially: *Brannigan v Commonwealth* (2000) 110 FCR 566.

16 See *Public Service Act 1999* (Cth) s 5; *Occupational Health and Safety Act 1991* (Cth) s 13(2); *Ombudsman Act 1976* (Cth) s 3C; *Crimes Act 1914* (Cth) s 3A. See *McDonald v Bojkovic* [1987] VR 287.

privacy of an individual.[17] The purpose of s 13D was said to be to ensure that 'the extra-territorial operation of the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs'.[18]

28.13 These acts and practices may be interferences with privacy, however, if they breach the Tax File Number (TFN) guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; breach Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or the data-matching guidelines; constitute a breach of the guidelines under s 135AA of the *National Health Act 1953* (Cth); or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[19]

28.14 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether there are any issues concerning overseas acts required by foreign law, and if so, how should they be dealt with.[20] This question elicited few comments from stakeholders. Civil Liberties Australia submitted that information about Australians should not be allowed to become the property of a foreign government, or be held under the laws of a foreign country.[21] The Office of the Privacy Commissioner (OPC) submitted that 'a note should be included under s 13D reminding organisations of their obligations in relation to transborder data flows of personal information under NPP 9'.[22]

28.15 The Office of the Victorian Privacy Commissioner (OVPC) noted the debate in Canada about whether medical information held in the United States might be subject to secret demands under the *Uniting and Strengthening America by Providing Appropriate Tools to Interact and Obstruct Terrorism Act 2001* (US) (*US Patriot Act*).[23]

28.16 In 2004, concerns were raised in Canada about whether organisations outside Canada, which were contracted to provide services to the federal and provincial governments, could be required to provide personal information about Canadian

---

17 See *Privacy Act 1988* (Cth) ss 6A(4), 6B(4), 13D(1).

18 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [65], [70].

19 *Privacy Act 1988* (Cth) s 13E.

20 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–8.

21 Civil Liberties Australia, *Submission PR 98,* 15 January 2007.

22 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

23 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007. Other examples include the handing over by Yahoo of a dissident journalist's email account details to the Chinese police in a matter that was the subject of investigation by the Hong Kong Privacy Commissioner; and the US Government mandating the transfer of passenger name records (PNRs) on all incoming international flight passengers. Issues were raised in relation to whether the release of PNRs was permitted under the EU Directive. The US and the EU have recently entered an agreement in relation to processing and transfer of PNRs. See *Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) 2007*.

citizens to the US authorities.[24] In response to these concerns, the Government of British Columbia amended the *Freedom of Information and Protection of Privacy Act 1996* (British Columbia) to provide that a government agency must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, except in certain circumstances.[25] The Canadian Government, by contrast, did not adopt a legislative approach to this issue. It developed a strategy that involved raising awareness and providing guidance about privacy risks associated with contracting with organisations outside Canada.[26]

28.17 Should the *Privacy Act* limit the circumstances when personal information transferred outside Australia will become subject to a foreign law? One option would be to amend s 13D to provide for certain limits. Another option is that reflected in the Trade Practices Amendment (Privacy Protection for Off-shoring) Bill 2007.[27] The Bill seeks to amend the *Financial Management and Accountability Act 1997* (Cth) by introducing a new s 43A which requires an agency entering into a Commonwealth contract for the provision of services in Australia to take contractual measures to ensure that a contracted service provider cannot undertake work in relation to the contract in a country other than Australia that would involve use of 'personally identifiable information'.[28] The Bill reflects one method of protecting personal information from being collected and held under the law of a foreign country.

28.18 The ALRC does not propose that s 13D of the *Privacy Act* be amended to limit the circumstances in which personal information transferred outside Australia will become subject to foreign law. The ALRC believes that the policy justification for s 13D is sound—acts and practices that take place in a foreign country, and are required by the laws of that country, generally should not be considered a breach of the Act.[29]

---

24 See Treasury Board of Canada, *Privacy Matters: The Federal Strategy to Address Concerns About the US PATRIOT Act and Transborder Data Flows* (2006); Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (2004).

25 *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 30.1. The Act also provides that the relevant government Minister is to be informed when a government agency or contracted service provider receives a foreign demand for disclosure: *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 30.2.

26 Treasury Board of Canada, *Privacy Matters: The Federal Strategy to Address Concerns About the US PATRIOT Act and Transborder Data Flows* (2006), Ch 3.

27 The Trade Practices Amendment (Privacy Protection for Off-shoring) Bill 2007 was introduced by the Hon Anna Burke MP into the Australian Parliament House of Representatives on 18 June 2007.

28 'Personally identifiable information' has the meaning set out in s 65AAAB of the *Trade Practices Act 1974* (Cth). The Bill introduces a new 65AAAB of the *Trade Practices Act*. It defines 'personally identifiable information' as information including: name, postal address, financial information, medical records, date of birth, phone number, email address, Medicare number, mother's maiden name, driver's licence number and tax file number. The ALRC notes that most of this 'information' would be 'personal information' under the *Privacy Act*.

29 Trade Practices Amendment (Privacy Protection for Off-shoring) Bill 2007 sch 1, cl 1.

28.19 The ALRC proposes that the OPC develop and publish guidance on the proposed 'Transborder Data Flows' principle. This should set out the steps to be taken when personal information transferred outside Australia may become subject to foreign law, including laws such as the *USA Patriot Act*. The guidance should also provide advice to agencies when contracting government services to organisations outside Australia.

28.20 The ALRC does not consider that a note should be included under s 13D reminding organisations of their obligations under the proposed 'Transborder Data Flows' principle. Such obligations relate to whether personal information can be sent overseas, while s 13D concerns the handling of personal information *after* the information has been sent overseas. Moreover, once s 13D applies, the *Privacy Act* does not.

National Privacy Principle 9

28.21 NPP 9 dictates the circumstances in which an organisation may transfer personal information it holds in Australia to someone in a foreign country. As with the other private sector provisions, it was introduced in 2000 as part of the extension of privacy principles to the private sector.[30]

28.22 NPP 9 prohibits the transfer by an organisation of an individual's personal information to someone in a foreign country (other than that individual or organisation) unless a number of conditions are satisfied.[31]

28.23 The principle is largely modelled on arts 25 and 26 of the EU Directive, which aim to ensure continued protection of personal information when data are sent from their originating country.[32] Where one of the conditions in (a)–(f) is satisfied, the Australian organisation transferring the data is not liable for subsequent privacy breaches. It is important, therefore, that these conditions are sufficiently stringent to prevent transfers that create unwarranted privacy risks.[33]

28.24 NPP 9 is limited to 'foreign countries' rather than 'other jurisdictions'. It does not protect personal information that is transferred to a state or territory government that is not subject to privacy law, or a private sector organisation that is exempt from

30 N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39, 42.

31 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 7.

32 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58; N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39, 8.

33 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 7.

the federal *Privacy Act*.[34] Where the transfer of personal information overseas is to the same organisation, not a third party, NPP 9 does not apply.

28.25 The *Privacy Act* was amended in 2004 to make it clear that the protection provided by NPP 9 applies equally to the personal information of Australian and non-Australian individuals.[35] This amendment was made by excluding NPP 9 from the citizenship and residency requirements of s 5B(1).

28.26 In IP 31, the ALRC asked whether NPP 9 provides adequate and appropriate protection for personal information transferred from Australia to a foreign country.[36] While some stakeholders submitted that NPP 9 provides adequate and appropriate protection,[37] others noted that NPP 9 is deficient in a number of respects, including: it does not address the transfer of personal information offshore by agencies; the perceived weakness of the tests for a 'reasonable belief' (NPP 9(a)) and the taking of 'reasonable steps' (NPP 9(f)); that organisations transferring data are not liable for any subsequent breaches; a lack of clarity as to how NPP 9 relates to other parts of the *Privacy Act*; and a lack of guidance for organisations as to what steps they must take to comply with NPP 9.[38] Each of these criticisms is dealt with in detail below.

Application of the 'Transborder Data Flows' principle to agencies

28.27 The *Privacy Act* does not regulate the transfer of personal information outside Australia by agencies. Some state and territory privacy legislation contains a transborder principle that regulates the public sector in that jurisdiction,[39] and a number of overseas jurisdictions impose obligations concerning transborder flows on both public and private sector bodies.[40]

Submissions and consultations

28.28 In IP 31, the ALRC asked whether the transfer of personal information offshore by agencies should be regulated by privacy principles.[41] A large number of stakeholders were in favour of extending NPP 9 to agencies.[42] For a number of

---

34 N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39, 8.

35 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [1-460].

36 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–1.

37 Law Council of Australia, *Submission PR 177,* 8 February 2007; ANZ, *Submission PR 173,* 6 February 2007.

38 Telstra, *Submission PR 185,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; AXA, *Submission PR 119,* 15 January 2007; Finance Sector Union, *Submission PR 109,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007;

39 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.

40 See, eg, *Data Protection Act 1998* (UK) s 63 and *Federal Data Protection Act 1990* (Germany) ss 1, 2.

41 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–31.

42 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Queensland Government, *Submission PR 242,* 15 March 2007; Office of the Privacy Commissioner,

stakeholders, the key issue was that 'personal information should not be transferred to a foreign jurisdiction unless the foreign jurisdiction offers privacy protections substantially similar to Australian privacy standards'.[43]

28.29 Several stakeholders pointed to the fact that technological developments, in conjunction with increased transnational cooperation, make it more important to regulate how government entities transfer personal information overseas. The OPC, for instance, stated:

> As national governments increasingly interact and cooperate in a vast array of areas such as health, immigration, law enforcement, and business, increasing amounts of personal information may be exchanged as part of these processes.[44]

28.30 A number of stakeholders supported the existence of a privacy principle regulating agencies in relation to transborder data flows, provided certain conditions were met. For instance, it was submitted that there should be a condition for the transfer of personal information if required or authorised by another piece of legislation,[45] or for the purposes of mutual assistance between governments.[46] Some stakeholders submitted that the principle should apply both to transfers across national borders, and across federal, state and territory borders.[47]

28.31 Other stakeholders opposed the application of such a privacy principle to agencies. The Australian Federal Police (AFP) submitted that its existing practices adequately balance the need to protect individuals' privacy with the need to transfer information as quickly as is required in any given situation.[48] It was also concerned that such a principle would have the effect of 'impos[ing] Australian privacy law onto offshore recipients of personal information from Australian agencies'.[49] The Australian Taxation Office suggested that agencies should be required to enter contractual

---

Submission PR 215, 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007.

43 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

44 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

45 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; CrimTrac, *Submission PR 158,* 31 January 2007.

46 CrimTrac, *Submission PR 158,* 31 January 2007.

47 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

48 Australian Federal Police, *Submission PR 186,* 9 February 2007.

49 Ibid.

arrangements obliging parties to whom they transfer information to respect the relevant privacy principles.[50]

ALRC's view

28.32 The *Privacy Act* should regulate the transfer of personal information outside Australia by agencies. Individuals should be assured that when an agency transfers personal information outside Australia their personal information will be protected to the same standard as under Australian privacy laws. The fact that agencies often have powers to compel the collection of personal information is a further reason for ensuring that personal information continues to be protected when it is transferred overseas. The ALRC also notes that the public sector in a number of Australian state and territory and overseas jurisdictions is regulated by a transborder data flow principle.[51]

28.33 The ALRC acknowledges, however, that a transborder data flow principle that applies to agencies will need to provide a condition for offshore transfers in certain circumstances, including transfers for the purpose of law enforcement, mutual assistance and extradition.[52] The *Personal Information Protection Act 2004* (Tas), *Information Act 2002* (NT) and the proposed Information Privacy Bill 2007 (WA) provide that a state or territory agency may transfer information outside that jurisdiction if the transfer is 'required or authorised by or under law'.[53] The *Privacy Act 1985* (Canada) provides that Canadian governmental bodies may not disclose the personal data of individuals without their consent, subject to a number of exceptions, including disclosures made

> under an agreement or arrangement between the Government of Canada or an institution thereof and … the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation.[54]

28.34 In the ALRC's view, the proposed 'Transborder Data Flows' principle should include a provision allowing an agency to transfer personal information outside Australia for law enforcement purposes. The condition should mirror the law enforcement exception under the proposed 'Use and Disclosure' principle. In the interest of clarity, the condition should also provide for the transfer of personal information for the purposes of extradition and mutual assistance.

28.35 The law enforcement condition proposed by the ALRC should not be worded as broadly as a 'required or authorised by or under law' condition under the proposed

---

50 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

51 See, eg, *Personal Data (Privacy) Ordinance* (Hong Kong) s 33(1); *Data Protection Act 1998* (UK) s 63; *Federal Data Protection Act 1990* (Germany) ss 1, 2.

52 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

53 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.

54 *Privacy Act* RS 1985, c P-21 (Canada) s 8(2)(f).

'Transborder Data Flows' principle. The ALRC is concerned that such a condition might be too permissive in the context of transfer to overseas jurisdictions that may not have a similar level of privacy protection to Australia. Further, such a condition could be interpreted as permitting uses and disclosures that would be authorised under the 'Use and Disclosure' principle. This would allow an agency or organisation to transfer information overseas in a range of circumstances currently not provided for by NPP 9.[55]

28.36 The ALRC is interested in views from stakeholders on whether the proposed 'Transborder Data Flows' principle requires further amendment to accommodate other acts and practices involving the transfer of personal information outside Australia by agencies.

Proposal 28–2 The proposed Unified Privacy Principles (UPPs) should contain a principle called 'Transborder Data Flows' that applies to agencies and organisations.

Proposal 28–3 The proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia if the transfer is necessary for one or more of the following by or on behalf of an enforcement body:

(a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(b) the enforcement of laws relating to the confiscation of the proceeds of crime;

(c) the protection of the public revenue;

(d) the prevention, detection, investigation or remedying of seriously improper conduct or proscribed conduct;

(e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(f) extradition and mutual assistance.

55 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996).

Definition of 'transfer'

28.37 The OPC submitted that it would be useful to distinguish the term 'transfer' from the terms 'use' and 'disclosure'. The OPC noted that the ordinary meaning given to the term 'transfer' is associated with information being sent somewhere. This may not be sufficient, however, to cover situations where personal information that is stored on a single server in one jurisdiction is available to be viewed and accessed in other jurisdictions.[56]

28.38 One option for dealing with this issue is to define 'transfer' in the Privacy Act as including the situation where personal information is stored in Australia in such a way that allows it to be accessed and viewed outside Australia. This definition would clearly capture the transfer of personal information on intranets and password-protected sections of websites. It also would include, however, uploading personal information on the internet. The ALRC is interested in hearing views on whether such a definition is appropriate.

28.39 Another issue is when an agency or organisation sends an email containing personal information by or to email systems that are hosted overseas.

> Imagine, for example, a situation where an Australia doctor emails some test results to an Australian patient. Imagine further that the patient is using Microsoft's Hotmail system. While the e-mail is sent from one Australian party to another, the e-mail including the sensitive personal information it contains, may be stored on a server overseas. Has the Australian doctor in this situation transferred personal information to someone in a foreign country? The answer would seem to be yes, as the information is placed on a server located in a foreign country.[57]

28.40 The Australian Government has dealt with this issue in the context of authorisations under the Integrated Public Number Database scheme.[58] Clause 4 of the *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* states that an authorisation is subject to a condition that prohibits the holder of an authorisation from transferring protected information to someone who is in a foreign country, subject to a number of exceptions. Clause 3(2) of the instrument provides that protected information is taken to be transferred to someone who is in a foreign country when 'it becomes accessible to the intended recipient of the information in the foreign country'. A note to cl 3 states that the clause

> is not intended to capture temporary offshoring of data such as when a document is emailed between 2 points within Australia but because of Internet routing it travels overseas on the way to its destination.

---

56 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

57 D Svantesson, *Protecting Privacy on the 'Borderless' Internet—Some Thought on Extraterritoriality and Transborder Data Flow* (2007) unpublished manuscript.

58 See discussion of the Integrated Public Number Database in Ch 63.

28.41 The ALRC is interested in views on whether the *Privacy Act* should provide that a 'transfer' excludes temporary transfer of data—such as when an email containing personal information is sent by or to an email system that is hosted overseas.[59]

Question 28–1 Should the *Privacy Act* provide that for the purposes of the proposed 'Transborder Data Flows' principle, a 'transfer':

(a) includes where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia; and

(b) excludes the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia?

'Someone' in a 'foreign country'

28.42 NPP 9 currently outlines when an organisation may transfer personal information about an individual to 'someone' who is in a 'foreign country'. A number of stakeholders submitted that NPP 9 should adopt the term 'person' as used in Note 3 to NPP 2 to clarify that the obligations under the Act with regard to disclosure of personal information outside of Australia apply to the release of personal information to organisations and government bodies as well as individuals.[60]

28.43 The OPC submitted, however, that rather than changing the term to 'person', a term such as 'recipient' would be preferable.[61] The OPC also submitted that consideration should be given to replacing the term 'foreign country' with 'outside Australia'. This will allow for a broader reading of what an overseas jurisdiction may include, for example, states and provinces and not only nation states.[62]

28.44 The ALRC proposes that NPP 9 should refer to the transfer of personal information to a 'recipient' rather than someone. This will make it clear that the principle applies to the overseas transfer of personal information to agencies, organisations and individuals. As discussed below, the note to the proposed 'Use and Disclosure' principle should also refer to 'recipient'. The ALRC also proposes that

---

59 Issues related to web-based applications are discussed in Ch 6.

60 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

62 Ibid.

NPP 9 be amended to refer to 'outside Australia' rather than to a 'foreign country'. 'Outside Australia' suggests a broader reading of what an overseas jurisdiction may be and also is consistent with language in overseas and state and territory transborder data principles.[63]

'Reasonably believes'

28.45 NPP 9(a) states that an organisation may transfer personal information to someone overseas where it 'reasonably believes' the recipient is subject to a law, binding scheme or contract that effectively upholds principles substantially similar to the NPPs. It has been argued that the requirement of a 'reasonable belief' is a weak test when compared to other models. In contrast, art 25 of the EU Directive provides that the country in question *must have* an adequate level of protection. Professor Graham Greenleaf has noted that NPP 9 only requires that an organisation reasonably believe that the foreign country has an arrangement that 'effectively upholds' privacy principles, not that there are enforcement mechanisms that are substantially similar to the *Privacy Act.*[64]

28.46 The OPC Guidelines to the NPPs state in relation to NPP 9:

> Given that transferring personal information overseas may remove it from the protection of Australian law, an organisation relying on NPP 9(a) and NPP 9(f) may need to be in a position to give evidence about the basis on which it decided that it has met the requirement of 'reasonable belief' or 'reasonable steps'.
>
> Getting a legal opinion would be a good way for an organisation to get such evidence.[65]

28.47 It is not clear what other action, if any, would be sufficient to satisfy the 'reasonable belief' requirement.

28.48 A number of submissions to the Inquiry noted that the concept of 'reasonable belief' is an ambiguous and weak test compared to the EU Directive requirement.[66] Other submissions argued that the 'reasonable belief' test should be retained and that the requirement under art 25 of the EU Directive is too onerous.[67] The OPC noted that it intends to develop information sheets outlining issues that should be addressed in

---

63 *Personal Data (Privacy) Ordinance* (Hong Kong) s 33(1); *Privacy and Personal Information Protection Act 1998* (NSW) s 19(2); *Information Privacy Act 2000* (Vic) sch 1, IPP 9; *Personal Information Protection Act 2004* (Tas) sch 2, PIPP 9; *Information Act 2002* (NT) sch 2, IPP 9.

64 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 8.

65 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58. See also J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5795].

66 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Finance Sector Union, *Submission PR 109,* 15 January 2007.

67 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

contractual agreements and how to assess more easily whether a privacy regime is 'substantially similar'.[68]

28.49 The ALRC does not propose the amendment of the 'reasonable belief' test. It is the ALRC's view, however, that the Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed Unified Privacy Principles (UPPs).[69] In the ALRC's view, this will go a long way to creating certainty about when the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles substantially similar to the NPPs.

28.50 The ALRC also proposes that the OPC should develop and publish guidance on the proposed 'Transborder Data Flows' principle. This should include guidance on what constitutes a 'reasonable belief'. Obtaining legal advice is one way this requirement could be satisfied.

Reasonable expectations of the individual

28.51 NPP 9(c) provides that an organisation may transfer personal information to someone overseas if the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request.

28.52 The OPC submitted that NPP 9(c) could be enhanced by an added specification that the transfer of personal information overseas should be 'within the reasonable expectations of the individual'. The OPC submitted that this would ensure that contracts or pre-contractual arrangements are clear about whether they may involve transfer of personal information overseas.[70]

28.53 The ALRC agrees that NPP 9(c) should be amended to provide that the transfer of personal information overseas should be within the reasonable expectations of the individual. Although an organisation or an agency may be acting on the request of an individual, the individual may not be aware that their request will require the transfer of their personal information outside Australia. In the ALRC's view, organisations and agencies should be required to specify in a contract or in pre-contractual arrangements that the fulfilment of the contract may require the overseas transfer of an individual's personal information.

---

68 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 18.

69 This issue is discussed further below, in the context of the role of the OPC. See Proposal 28–8.

70 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

Interests and benefit of the individual

28.54 NPP 9(d) states that an organisation may transfer personal information to someone overseas if the transfer is necessary for the conclusion or performance of a contract concluded 'in the interest of the individual' between the organisation and a third party. NPP 9(e) provides that an organisation may transfer personal information to someone overseas if all of the following apply: the transfer is 'for the benefit of the individual'; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it.

28.55 It was submitted that these conditions are unclear, difficult to apply in practice,[71] and have led to 'an inconsistent approach with respect to transborder data flow that undermines consumer confidence'.[72] The OPC submitted that:

> Given that the reason for off-shoring the information might be based on organisational efficiency, judgements regarding the benefit to or interests of an individual may be difficult for an organisation to make.[73]

28.56 The ALRC does not propose the removal of the requirements in NPP 9(d) and (e) that a contract is in the 'interest of the individual' or that the transfer is for the 'benefit of the individual'. These requirements provide important protections for the data subject. The ALRC acknowledges, however, that these requirements involve subjective assessments. To assist agencies and organisations make these assessments, the ALRC proposes that the OPC develop and publish guidance on the proposed 'Transborder Data Flows' principle, which addresses when a transfer of personal information is for the benefit or in the interests of the individual concerned.

28.57 In the ALRC's view, where the reason for a transfer is organisational efficiency, the transfer should only take place if one of the other conditions in the proposed 'Transborder Data Flows' principle is satisfied. For example, the organisation or agency may need to take reasonable steps before the transfer has taken place to ensure that the information will not be handled by the recipient of the information inconsistently with the proposed UPPs.

'Reasonable steps'

28.58 Under NPP 9(f), personal information may be transferred to a foreign country where the organisation has taken 'reasonable steps' to ensure that the information transferred will not be held, used or disclosed by the recipient of the information inconsistently with the NPPs. This exception has been criticised as 'weak and imprecise' because it does not allow an individual recourse where an organisation has

---

71 Ibid; Telstra, *Submission PR 185,* 9 February 2007.
72 Telstra, *Submission PR 185,* 9 February 2007.
73 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

not adequately fulfilled the 'reasonable steps' requirement.[74] There is also an issue about the propriety of allowing, as a stand-alone exception, an organisation, without qualification, to transfer personal information about an individual and *then* to take reasonable steps to ensure that the recipient will not deal with it inconsistently with the NPPs.[75]

28.59 In IP 31, the ALRC noted that it may be preferable for NPP 9 to articulate the general principle that an organisation may transfer personal information if, *before* the transfer has taken place, it has taken reasonable steps to ensure that the recipient will not hold, use or disclose it inconsistently with the NPPs. An exception to that principle could be to allow the organisation to transfer the information and take the requisite reasonable steps after transfer only in exceptional circumstances or specified circumstances—such as an emergency or for a law enforcement purpose—or where it was not practicable to take such steps.[76]

28.60 Submissions were generally supportive of amending NPP 9(f) to require that 'reasonable steps' to be taken *before* personal information is transferred.[77] The OPC submitted that organisations may require further guidance on what constitutes 'reasonable steps' in this clause.

> The Office considers that when an organisation does not have an understanding of the privacy regime operating in the recipient's jurisdiction, a 'reasonable step' for the organisation is to ensure that privacy protections equivalent to the NPPs are in place through contracts. The Office suggests that it work with business to develop guidance material that explains what 'reasonable steps' might include.[78]

28.61 In the ALRC's view, NPP 9(f) provides little guarantee that personal information will be protected when it is transferred outside Australia. Once an organisation has transferred the information it has lost control over it. Allowing this stand-alone exception appears to go against the general spirit of NPP 9, which is to ensure that there are adequate protections *before* transfer takes place. The ALRC therefore proposes that *before* a transfer takes place, an agency or organisation must take reasonable steps to ensure that the information will not be handled by the recipient of the information inconsistently with the proposed UPPs. The ALRC also proposes

---

74 G Greenleaf, 'Exporting and Importing Personal Data: The Effects of the Privacy Amendment (Private Sector) Bill 2000' (Paper presented at National Privacy and Data Protection Summit, Sydney, 17 May 2000), 8. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

75 As well as under the *Privacy Act 1988* (Cth), this is also the position in relation to transfers of personal information outside of Victoria, Tasmania, and the Northern Territory: *Information Privacy Act 2000* (Vic) sch 1, IPP 9.1(f); *Health Records Act 2001* (Vic) sch 1, Health Privacy Principle 9.1(f); *Personal Information Protection Act 2004* (Tas) sch 1, Personal Information Protection Principle 9(d); *Information Act 2002* (NT) sch, IPP 9.1(g).

76 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [13.24].

77 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

78 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

that guidance on the proposed 'Transborder Data Flows' principle should include advice on what constitutes 'reasonable steps'.

28.62 Only one submission addressed the need for a provision dealing with exceptional or specified circumstances and did not specify what those circumstances should include.[79] The ALRC is interested in hearing from other stakeholders about this issue.

Accountability

28.63 Professor Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that the six conditions under NPP 9 will generally be sufficient to allow any legitimate transfer overseas of personal information, even when those transfers may harm the interests of the data subjects concerned. It was submitted that data exporters should remain liable for breaches of privacy by data importers under most circumstances.[80]

28.64 The Australian Government Department of Communications, Information Technology and the Arts (DCITA) noted the inherent difficulties in imposing legal responsibility upon an overseas recipient of personal information to use or disclose that information in a manner that is consistent with the NPPs. While contractual arrangements may assist in this regard, the OPC could still only take action against the Australian-based transferer of the information, should such information be used or disclosed inappropriately outside of Australia.[81]

28.65 One option for addressing these problems is to amend the *Privacy Act* to introduce an 'accountability' concept in the proposed 'Transborder Data Flows' principle. This could be achieved by providing that agencies and organisations will continue to be liable for any breaches of the proposed UPPs when an individual's personal information is transferred outside Australia.

28.66 As discussed below, the APEC Privacy Framework provides that, once an organisation has collected personal information, it remains accountable for the protection of that personal information even if the information changes hands or moves from one jurisdiction to another.[82] Similarly, Principle 12 of the Asia-Pacific Privacy Charter provides that an organisation must not transfer personal information to a place outside the jurisdiction in which it is located unless a number of conditions are met, including that the organisation has taken all reasonable steps to ensure that the personal information will be dealt with in accordance with the Asia-Pacific Privacy Charter

---

79 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

80 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

81 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

82 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 9.

Principles in that place and the organisation continues to be liable for any breaches of the Principles.

28.67 Another example is Principle 4.1.3 of the *National Standard of Canada Model Code for the Protection of Personal Information* (Canada) (Model Code). That principle provides that an organisation is responsible for personal information in its possession or custody, including information that has been transferred overseas to a third party for processing.[83] Organisations, therefore, must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[84]

28.68 There are several advantages to such an accountability principle. Placing liability on the agency or organisation transferring the personal information ensures that an individual has the ability to seek redress from someone in Australia if the recipient breaches the individual's privacy. Although this appears to be onerous, agencies and organisations can mitigate their liability in contractual arrangements with the recipient of the personal information. Further, the individual will be able to approach a local regulator, rather than have to seek protection under a foreign law, which may not provide the same level of protection as a local law.

28.69 To what extent should agencies and organisations remain liable when transferring personal information overseas? In the ALRC's view, an agency or organisation should not be liable for the handling of personal information after it has been transferred to another entity when the individual in question consents to the transfer. Where an individual has exercised choice over where his or her information will be transferred and the level of protection it will receive, the individual should bear the consequences of the transfer.

28.70 Agencies and organisations should not remain accountable when they reasonably believe that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs. In these circumstances, the personal information will receive similar protection to that under the *Privacy Act*. The individual can seek redress under a law, scheme or contract that is substantially similar to the proposed UPPs if the recipient of the personal information mishandles that information.

28.71 An agency should not be liable for the transfer of personal information if it is necessary for law enforcement purposes. In many cases, an agency will have no choice but to transfer information overseas, for example, for the purpose of a police investigation or the extradition of a person.

---

83 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 5.

84 D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 923.

28.72 In conclusion, an agency or organisation should be permitted to transfer personal information to a recipient in Australia provided that: (1) the agency or organisation remains liable for any breach of the privacy principles; and (2) one of the following conditions is satisfied:

- the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;

- the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

- all of the following apply: the transfer is for the benefit of the individual; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

- before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.

Proposal 28–4 Subject to Proposal 28–3, the proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia only if at least one of the following conditions is met:

(a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs; or

(b) the individual consents to the transfer; or

(c) the agency or organisation continues to be liable for any breaches of the proposed UPPs; and

(i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;

(ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

(iv) all of the following apply: the transfer is for the benefit of the individual; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

(v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.

Interaction with the 'Use and Disclosure' principle

28.73 Under the NPPs, an organisation that wants to transfer personal information outside Australia needs to determine whether the disclosure of that information to someone outside Australia will comply with NPP 2 (the Use and Disclosure principle). The organisation then needs to determine whether the transfer will satisfy at least one of the conditions set out under NPP 9. In the ALRC's view, this should continue to be the case under the proposed UPPs in relation to both agencies and organisations.

28.74 In the interest of clarity, the ALRC proposes that the proposed 'Use and Disclosure' principle should contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia. The proposed 'Transborder Data Flows' principle should also contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

Proposal 28–5 The proposed 'Use and Disclosure' principle should contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

Proposal 28–6 The proposed 'Transborder Data Flows' principle should contain a note stating that agencies and organisations are subject to the requirements of the proposed 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

Related bodies corporate

28.75 NPP 9 does not prevent transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned.[85] As noted above, the *Privacy Act* operates extra-territorially in these circumstances by virtue of s 5B.

28.76 A company transferring personal information overseas to another related company, however, must comply with NPP 9. Section 13B(1) states that an act or practice is not an interference with the privacy of an individual if it involves a body corporate collecting or disclosing personal information (that is not sensitive information) from or to a related body corporate. A 'related body corporate' is a body corporate that is: a holding company of another body corporate; a subsidiary of another body corporate; or a subsidiary of a holding company of another body corporate; and the first mentioned body and the other body are related to each other.[86]

28.77 In submissions to the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review), a number of stakeholders called for clarification of the interaction between NPP 9 and s 13B(1). They argued that it was unclear whether s 13B(1) made it possible for a body corporate in Australia to transfer personal information to a related body corporate located outside Australia without reference to NPP 9.[87]

28.78 In its final report, the OPC observed that s 13B relates to the purposes for which information can be disclosed, whereas NPP 9 is concerned with whether information can be sent overseas. While s 13B(1)(b) enables disclosure of information, compliance with NPP 9 is still required for transfers of information to a foreign country.

---

85 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58.

86 This definition is from the *Corporations Act 2001* (Cth) s 50, as referred to in s 6(8) of the *Privacy Act 1988* (Cth). For a general discussion of the exemption, see Ch 39.

87 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 77.

> If a company has an organisational link with Australia under section 5B, the extra-territorial provisions in the *Privacy Act* will apply. Therefore, if personal information is sent overseas to the same company, it will continue to be protected by the *Privacy Act* because the extra-territorial provisions apply. Section 5B does not appear to apply to related entities outside of Australia. As such, if information is sent to a related company, it may not be protected by the *Privacy Act*.[88]

28.79 The OPC took the view that, where information is transferred outside of Australia and the extraterritorial provisions do not apply, it is in the public interest for NPP 9 to apply. The OPC therefore did not recommend excluding related corporations from having to comply with NPP 9.[89]

28.80 In its submission to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry), the Australian Privacy Foundation (APF) argued that s 13B was complex, difficult to understand and 'too generous in allowing exchanges of information between related companies which effectively avoid some of the NPP obligations'.[90] It stated further:

> If businesses choose for their own reasons to structure their affairs through separate incorporations, we do not see why this should give them any exemption from the normal application of the NPPs.[91]

28.81 The APF argued that the exemption under s 13B should be removed and that related companies should be treated as third parties.[92]

28.82 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate.[93] A number of stakeholders submitted that the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, this transfer will be subject to NPP 9.[94]

28.83 Other stakeholders submitted, however, that NPP 9 should not apply when personal information is transferred outside Australia to a related body corporate.[95] For

---

88 Ibid, 79.
89 Ibid, 79.
90 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.171].
91 Ibid, [4.171].
92 Ibid, [4.171].
93 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–2.
94 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
95 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007.

example, Microsoft Australia submitted that transborder data flows to related bodies corporate that operate under a common set of internal polices, which require adherence to privacy notices and consent provided by individuals, should not be regulated in the same way as international transfers of personal information to unrelated third parties.[96]

28.84 In the ALRC's view, NPP 9 should apply to transborder transfers to related bodies corporate. If personal information is sent overseas to the same company, it will continue to be protected by the *Privacy Act* because the extra-territorial provisions apply. Section 5B does not apply, however, to related bodies corporate outside of Australia. As such, if personal information is sent to a related company, it may not be protected by the *Privacy Act*. Although many related companies are governed by a common set of internal policies, this may not always be the case. Further, the internal policies of a related company may not always provide the same level of protection as the *Privacy Act*. The ALRC agrees with the OPC that, where information is transferred outside of Australia and the extraterritorial provisions do not apply, it is in the public interest for NPP 9 to apply.

Proposal 28–7 Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, this transfer will be subject to the proposed 'Transborder Data Flows' principle.

The role of the Privacy Commissioner

List of overseas jurisdictions

28.85 The *Privacy Act* does not provide a definition of what constitutes a 'substantially similar' set of principles for the purposes of NPP 9(a).[97] The OPC Review noted that stakeholders had expressed frustration at the lack of guidance regarding the countries whose laws provide adequate protection equivalent to the NPPs.

> In this situation the onus is on the organisation to assess the regime of the country in which their trading partner resides. Many stakeholders, especially small businesses, have criticised the efficiency of this system arguing that they neither have the expertise or the resources to assess a foreign country's privacy laws.[98]

28.86 It was suggested that the OPC could publish a list of countries with substantially similar privacy laws. This would give organisations greater certainty about the countries to which they could transfer information safely. The OPC rejected this

96 Microsoft Australia, *Submission PR 113,* 15 January 2007.
97 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2-5800].
98 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

proposal on the basis that it was a complex task that would require considerable resources. The OPC also argued that such a task could affect its relationships with other countries and may be an inappropriate task for it to undertake.[99]

28.87 An alternative view is that, if assessment of a country's privacy compatibility is complex, a central body of experts should be tasked with assessing these regimes. As previously noted, the OPC has suggested that an organisation seek legal advice to ensure that it has evidence to meet the requirement of 'reasonable belief' or 'reasonable steps'.[100]

28.88 In its submission to the House of Representatives Committee on Legal and Constitutional Affairs inquiry into the Privacy Amendment (Private Sector) Bill 2000 (Cth), the European Commission made a similar point. It argued that 'it is our experience that it is difficult for the average operator to have substantial knowledge of the level of protection of personal data in third countries'.[101]

> Exonerating an operator of all responsibility under the Act simply by applying a reasonable belief test is likely to create uneven conditions for data transfers outside Australia. Also, the existence of a law, a contract or binding scheme is, in itself, an objective fact that can be ascertained, hence the reasonable belief test is somewhat unsettling. We believe that in this instance, the assistance of the Privacy Commissioner in indicating what third country regime can be considered as substantially similar to your domestic situation is advisable.[102]

28.89 In IP 31, the ALRC asked what role, if any, the OPC should play in identifying countries that have protection for personal information equivalent to the *Privacy Act*.[103] The vast majority of submissions in response to this question stated that the OPC should assist organisations with their decisions under NPP 9 by publishing and maintaining a list of countries that satisfy this provision.[104] Submissions noted that this would assist individuals to make choices about the handling of personal information, and businesses to make decisions about when alternative arrangements are needed to protect personal information.[105]

---

99 Ibid, 79.

100 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 59.

101 European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000), 7.

102 Ibid, 7.

103 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–3.

104 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

105 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI,

28.90 Submissions also noted that the OPC would be assisted in assessing overseas jurisdictions by the work of the European Union (EU) Article 29 Data Protection Working Party,[106] and could work with the Australian Government Department of Foreign Affairs and Trade.[107] The Law Council of Australia submitted that the OPC or a panel of experts should develop the list.[108] Another stakeholder noted that the best compromise would be to empower, but not require, the OPC to operate a 'whitelist' of countries with equivalent laws.[109]

28.91 It was submitted that publishing a list of countries with substantially similar privacy laws may not be an appropriate task for the OPC.[110] The OPC reiterated its view that such a task would be complex, require considerable resources, and could affect its relationships with other countries.[111] The OVPC submitted that these types of decisions are best left to governments acting with the advice of privacy commissioners.[112]

28.92 In the ALRC's view, the benefits of developing a list of laws and binding schemes that have equivalent *Privacy Act* protection for personal information far outweigh any disadvantages. Stakeholders have clearly identified the need for a list on a number of occasions.[113] Such a list would assist agencies and organisations to comply with the proposed 'Transborder Data Flows' principle. Further, it would assist individuals to make choices based on where their personal information may be transferred, and how it will be handled.

28.93 The ALRC accepts that this task would have considerable resource implications for the OPC. The ALRC therefore proposes that the Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed UPPs. This may be a suitable task for the Australian Government Attorney-General's Department, in consultation with other Australian Government agencies such as the Department of Foreign Affairs and Trade and the OPC.[114]

Submission PR 147, 29 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

106 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

107 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

108 Law Council of Australia, *Submission PR 177,* 8 February 2007.

109 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

110 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

111 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

112 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

113 See, eg, European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

114 The ALRC notes that Ernst & Young have compiled such a list: Ernst & Young, *Data Protection in the European Union and Other Selected Countries: A New Comparative Study* (2006).

Proposal 28–8 The Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed UPPs.

Contractual arrangements

28.94 The final report of the OPC Review notes that:

> From submissions and the comments received during stakeholder workshops, it appears that organisations are fulfilling their NPP 9 obligations of ensuring that personal information is protected when it is transferred to regions without privacy regimes through contractual arrangements with their trading partners. While some submissions find this to be an effective solution, others are concerned about the costs associated with monitoring the compliance of their trading partners.[115]

28.95 For example, Telstra submitted to the OPC Review that it uses contractual provisions in its agreements with third party suppliers to manage the flow of personal information overseas, and imposes contractual obligations on overseas suppliers to ensure Telstra complies with its obligations under NPP 9. Some concerns were raised, however, regarding the additional cost of this method of ensuring compliance.[116]

28.96 The final report of the OPC Review notes that the OPC could provide greater guidance by publishing approved standard contractual provisions for use by Australian companies and international trading partners.

> These contractual provisions could provide for how the international company must protect information when the information collected in Australia is transferred to organisations overseas. The EU has issued contract provisions. Developing standard contractual provisions would have resource implications for the Office.[117]

28.97 Rather than publishing standard contractual provisions, the OPC recommended that it provide further guidance to assist organisations in complying with NPP 9. The OPC suggested issuing an information sheet outlining the issues that should be addressed as part of a contractual agreement and how to assess whether a privacy regime is substantially similar.[118]

---

115 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78 (footnotes omitted).

116 Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

117 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

118 Ibid, rec 18.

28.98 Some submissions to this Inquiry noted that it would be helpful if the OPC developed voluntary model contractual clauses in consultation with organisations as an aid to compliance with NPP 9, particularly for small to medium businesses.[119]

28.99 NPP 9 and the proposed 'Transborder Data Flows' principle anticipate that organisations will use contracts to protect personal information when it is transferred outside Australia. In the ALRC's view, the OPC should therefore develop and publish guidance about the issues that should be addressed as part of such a contractual agreement. This guidance will be particularly helpful for small businesses. The ALRC notes that the OVPC has published *Model Terms for Transborder Data Flows of Personal Information*. The guide includes model clauses for the transfer of personal information outside Victoria, together with commentary about the clauses.[120]

28.100 In other sections of this chapter, the ALRC proposes that guidance on the proposed 'Transborder Data Flows' principle also should address:

- when personal information may become available to a foreign government;
- contracting out government services to organisations outside Australia;
- when a transfer of personal information is 'for the benefit' or 'in the interests of' the individual concerned; and
- what constitute 'reasonable steps' to ensure the information it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the proposed UPPs.

Proposal 28–9 The Office of the Privacy Commissioner should develop and publish guidance on the proposed 'Transborder Data Flows' principle, including guidance on:

(a) when personal information may become available to a foreign government;

(b) outsourcing government services to organisations outside Australia;

(c) the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal information;

---

119 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007.

120 Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information* (2006).

(d) when a transfer of personal information is 'for the benefit' or 'in the interests of' the individual concerned; and

(e) what constitute 'reasonable steps' to ensure the information it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the proposed UPPs.

Cross-border enforcement

28.101 The ability to investigate breaches of local privacy laws in foreign countries poses particular challenges for privacy regulators.[121] The OECD identified considerable scope for a more global and systematic approach to cross-border privacy law enforcement cooperation.[122]

28.102 Cross-border cooperation of privacy regulators will be essential in enforcing the proposed 'Transborder Data Flows' principle. The ALRC notes that the OPC is already involved in a number of forums aimed at improving cooperative arrangements between privacy regulators in other jurisdictions. For example, the OPC is a member of the Asia Pacific Privacy Authorities Forum (APPA). APPA meets biannually and includes the federal, state and territory privacy regulators of Australia, New Zealand, Hong Kong and South Korea. APPA's objectives include: facilitating the sharing of knowledge and resources between privacy authorities within the region; fostering cooperation in privacy and data protection; promoting best practice amongst privacy authorities; and working to improve performance to achieve the objectives set out in privacy laws of each jurisdiction.[123]

28.103 The Australian Government, including the OPC, is also involved in the implementation of the APEC Privacy Framework. This will involve cooperation between regulators in APEC economies.[124]

28.104 The OPC has also entered into an agreement with the New Zealand Privacy Commissioner that allows for cooperation on privacy related issues. The Memorandum of Understanding covers the sharing of information related to surveys, research projects, promotional campaigns, education and training programs, and techniques in investigating privacy violations and regulatory strategies. Other areas addressed include cooperation on complaints with a cross-border element and the possible undertaking of joint investigations. The ALRC encourages the Australian Government

---

121 See, eg, *Lawson v Accusearch Inc* (2007) (Federal Court of Canada, Harrington J, 5 February 2007).

122 Organisation for Economic Co-operation and Development, *Report on the Cross-Border Enforcement of Privacy Laws* (2006), 4.

123 Asia Pacific Privacy Authorities Forum, *Statement of Objectives* (2005).

124 See, eg, *Second Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework*, Cairns, 25–26 June 2007.

and the OPC to continue to seek opportunities for further cooperation with privacy regulators outside Australia.

Requirement of notice that personal information is being sent overseas

28.105 As noted above, a large number of respondents to the ALRC's National Privacy Phone-in expressed concerns about Australian companies sending their personal information overseas. The OPC Review also noted that, for many consumers, 'the transfer of personal information overseas brings with it a perceived loss of privacy and control'.[125]

28.106 In its submission to the OPC Review, Electronic Frontiers Australia expressed the view that

> the NPPs should be amended to require organisations to give individuals notice that their information will be sent to a foreign country and that the individual will be required to deal with call centres located in a foreign country.[126]

28.107 As part of this notice, Electronic Frontiers Australia argued that organisations also should be required to inform individuals of the means by which the Australian organisation has ensured that the individual's personal information will be adequately protected. Such notice would not be required if the overseas organisation is subject to substantially similar privacy laws or the individual has consented to the transfer.[127] This suggestion was not discussed further in either the OPC Review or the Senate Committee privacy inquiry.

28.108 In July 2006, United States (US) Senator Hillary Clinton put forward a similar proposal in her privacy Bill, known as the Privacy Rights and Oversight for Electronic Commercial Transactions Act of 2006.[128] Under cl 10(b)(1), a business may not disclose personal information regarding a US resident to any foreign branch, affiliate, subcontractor, or unaffiliated third party located in a foreign country unless the company notifies each individual concerned and the individual is given an explanation and the opportunity to opt out of having his or her information transferred. This clause is designed to stop perceived losses in consumer protection where companies send their data for processing in overseas jurisdictions.

> This would have two benefits: again, putting the control of information in your own hands, but also sending the message to other countries that if they want to continue

---

125 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.

126 Ibid, 78.

127 Ibid, 79.

128 The text of the Bill may be viewed at <www.theorator.com/bills109/s3713.html> as at 31 July 2007. The Bill has been sent to the Senate Judiciary Committee for consideration.

> employing people in this very lucrative, rapidly growing area of information handling, they need to strengthen their own laws.[129]

28.109 This aspect of the Bill has been criticised as imposing an unnecessary burden on business. In the US context, the example was cited of a company with data processing centres in the US and Canada. If the US system broke down, for example, there would be delays involved in sending the data to the Canadian system for processing because of the requirement to inform consumers and allow them the opportunity to opt out.[130]

28.110 A similar Bill has been introduced by the Australian Labor Party.[131] The proposed new provisions would make it an offence if a corporation discloses 'personally identifiable information' to any branch, affiliate, subcontractor, or unaffiliated third party located in a country other than Australia unless: the corporation provides notice; and the consumer is given the opportunity, before the time that such information is initially disclosed, to object to the disclosure of such information. The Bill provides that, at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a corporation must provide a clear and conspicuous disclosure to the consumer in writing or in electronic form of the corporation's policies and practices with respect to the transmission of personally identifiable information.[132]

Submissions and consultations

28.111 In IP 31, the ALRC asked whether organisations should be required to inform individuals that their personal information is to be transferred outside Australia, and if so, what form such notification should take.[133]

28.112 Most stakeholders agreed that individuals should be informed that their personal information is to be transferred outside Australia. Some submissions argued that there also should be a requirement to inform individuals of the jurisdiction to which their personal information is to be transferred, so that individuals can exercise informed choice or bring pressure for improvements in legislative protection.[134] Other stakeholders submitted that transfer of personal information should only occur with

---

129 H Clinton, *Remarks of Senator Hillary Rodham Clinton on Privacy to the American Constitution Society: 16 June 2006* (2006) Senator Clinton's Website <clinton.senate.gov/news/statements/details.cfm?id=257288&> at 31 July 2007.

130 K Magill, 'Hillary's Privacy Bill a Whopper', *Direct Magazine* (online), 5 September 2006, <directmag.com/news/hillary_privacy_bill>.

131 See the Trade Practices Amendment (Privacy Protection for Off-shoring) Bill 2007 (Cth), which introduces a new Part V Division 1AAAA of the *Trade Practices Act 1974* (Cth).

132 Trade Practices Amendment (Privacy Protection for Off-shoring) Bill 2007 sch 1, cl 2.

133 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–4.

134 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007.

consent,[135] and that general notification (for example, by a notice on the collecting organisation's website) is insufficient.[136]

28.113 The form in which the notice is given is relevant to the burden placed on business and government. There is an enormous cost difference depending on whether notice has to be given to each individual or whether it could be posted, for example, on a company's website. Some stakeholders submitted that a requirement to notify individuals of a decision to transfer personal information overseas, where this was not foreshadowed at the time of collection, would place an unnecessary burden on transborder data flows and create an unjustified compliance burden.[137] It was noted that, for large companies, the cost of complying with the requirement to give notice could run to millions of dollars. Some stakeholders suggested, however, that if an organisation intends to transfer the data at the time of collection, notification should be given at that point. If the organisation later decides to export the data, it should give notice at that time.[138]

28.114 The Finance Sector Union submitted that its research has shown that consumers believe their data should not be transferred or accessed from overseas without their written permission, and support a legislative regime that would require financial institutions to disclose whether they store customer information overseas. The Union also submitted that notification should include the legal basis on which personal information will be transferred.[139]

28.115 A number of submissions noted that the *Privacy Act* already provides adequate protection of personal information that is transferred overseas. It was noted that NPP 1.3 requires organisations to take reasonable steps to ensure that an individual is aware of the organisations or types of organisations to which personal information might be disclosed. This could include overseas organisations.[140]

28.116 The OPC stated that it would be clearer for individuals and organisations if notification of overseas transfers was an explicit requirement within the NPPs. This

---

135 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; Finance Sector Union, *Submission PR 109,* 15 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007.

136 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.

137 See, eg, Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; ANZ, *Submission PR 173,* 6 February 2007; AXA, *Submission PR 119,* 15 January 2007.

138 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

139 Finance Sector Union, *Submission PR 109,* 15 January 2007.

140 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

could be done as part of the usual notice procedures. The OPC also noted that a requirement to provide notice to individuals should apply regardless of whether the overseas organisation is a related body corporate of its Australian parent or an agent or contractor of an Australian organisation. The OPC also submitted that, if an organisation has not previously needed to transfer personal information outside Australia but circumstances have changed since the information was collected, the organisation should notify affected customers.[141]

28.117 Some stakeholders also suggested that, in addition to providing notice of the transfer, organisations could provide further information about transfers of personal information outside Australia in their privacy policy or at the request of the individual.[142]

ALRC's view

28.118 In the ALRC's view, if personal information will, or may, be transferred outside Australia, agencies and organisations should be required to notify individuals. This would help individuals to exercise informed choice about how their personal information will be dealt with, and the level of privacy protection it will receive. In the ALRC's view, however, requiring notification or written consent each time an agency or organisation transfers an individual's personal information overseas would result in an unjustified compliance burden.

28.119 The proposed 'Specific Notification' principle would require an agency or organisation that collects personal information about an individual from the individual, to take reasonable steps to ensure that the individual is aware of a number of matters, including types of people, organisations, agencies or other entities to which the agency or organisation usually discloses personal information.[143] The requirement would extend to notifying an individual if his or her personal information might be transferred outside Australia.

28.120 Further, the ALRC proposes, in Chapter 21, that the proposed 'Openness' principle should require agencies and organisations to create a Privacy Policy that sets out their policies on the management of personal information.[144] In the ALRC's view, this Privacy Policy should set out whether personal information will be transferred outside Australia. If an agency or organisation's policy changes on transfer of personal information outside Australia, the Privacy Policy should be updated to reflect this.

---

141 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

142 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; ANZ, *Submission PR 173,* 6 February 2007.

143 Proposal 20–2.

144 Proposal 21–1.

Proposal 28–10 The Privacy Policy of an agency or organisation, referred to in the proposed 'Openness' principle, should set out whether personal information may be transferred outside Australia.

International privacy protection

28.121 In order to ensure that Australian organisations are not disadvantaged in the international market, Australia must be able to meet the international community's expectations of privacy protection. This section of the chapter considers the adequacy of Australia's privacy laws in relation to the EU Directive, and other international instruments such as the APEC Privacy Framework. It also considers various other international models of transborder data flow protection.

European Union Data Protection Directive

28.122 The EU Directive seeks to protect the privacy of individuals within the EU when information about them is transferred to countries outside the EU.[145] If the European Commission determines that a country does not provide 'adequate' data protection standards, this will lead to restrictions on the transfer of information to that jurisdiction.[146]

28.123 Article 25(1) of the EU Directive provides:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

28.124 Article 25(4) provides:

> Where the Commission finds … that a country does not ensure an adequate level of protection … Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

28.125 Article 26 provides an exception to art 25, permitting transfers in certain circumstances to a third country, even where the third country has not ensured an adequate level of protection. The art 26 exception applies in similar (though not identical) circumstances to those referred to in NPP 9—that is, where:

- there is unambiguous consent from the data subject;

---

145 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

146 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 9.

- the transfer is necessary for the performance, implementation or conclusion of certain contractual transactions;

- the transfer is in the public interest or the vital interests of the data subject; or

- the transfer is made from a public register.

28.126 Under art 26(2), a member state may also authorise transfers of personal data where a contract contains adequate safeguards protecting the 'privacy and fundamental rights and freedoms of individuals, and as regards the exercise of corresponding rights'.[147]

28.127 The decision about the adequacy of third party regimes is made by the Article 29 Data Protection Working Party of the European Commission (Working Party), which is comprised of representatives of supervisory authorities in EU member states and a representative of the European Commission. Those countries that have been declared 'adequate' are: Canada, Switzerland, Argentina, Guernsey and the Isle of Man. The US Department of Commerce's Safe Harbour Privacy Principles also have been given adequacy status.[148]

28.128 The Working Party has noted that 'adequate protection' does not necessarily mean equivalent protection, and that it is not necessary for third countries to adopt a single model of privacy protection. It has also stated that there may be adequate protection despite certain weaknesses in a particular system 'provided, of course, that such a system can be assessed as adequate overall—for example, because of compensating strengths in other areas'.[149]

28.129 If a third country is deemed not to have adequate protection, member states must take action to prevent any transfer of personal data to the country in question. This 'mandated approach' is stronger than that set out in the OECD Guidelines.[150]

28.130 Professors Colin Bennett and Charles Raab note that the implementation of arts 25 and 26 pose problems for businesses that rely on transborder flows of personal data. This matter also has major implications for credit-granting and financial institutions, hotel and airline reservations systems, the direct marketing sector, life and property insurance, the pharmaceutical industry, and for any online company that markets its products and services internationally.[151]

---

147 See discussion of the use of contracts for compliance with the EU Directive below.

148 See European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Information in Third Countries* <ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm> at 31 July 2007.

149 Text on Non-Discrimination adopted by the Article 31 Committee (31 May 2000), cited in D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed, 2006), 935.

150 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), 99.

151 Ibid, 99.

Adequacy of the Privacy Act

28.131 One of the main drivers behind the *Privacy Amendment (Private Sector) Act 2000* (Cth) was to facilitate trade with European countries by having the *Privacy Act* deemed adequate for the purposes of the EU Directive.[152] In March 2001, however, the Working Party released an opinion expressing concern that some sectors and activities are excluded from the protection of the *Privacy Act*, including small businesses and employee records.[153] The Working Party found that, without further safeguards, the Australian standards could not be deemed equivalent to the EU Directive. The Working Party also expressed concerns about Australia's regulation of sensitive information within the *Privacy Act* and the lack of correction rights, which existed for EU citizens under the Act.[154]

28.132 Further amendments were made to the *Privacy Act* in April 2004 as part of the process of moving towards adequacy.[155] Those amendments:

- clarified that the protection offered by NPP 9 applies equally to the personal information of Australians and non-Australians;
- removed nationality and residency limitations on the power of the Privacy Commissioner to investigate complaints regarding the correction of personal information; and
- gave businesses and industries more flexibility in developing privacy codes that cover otherwise exempt acts.[156]

28.133 The OPC Review noted that there are ongoing discussions with the European Commission regarding the small business and employee records exemptions from the *Privacy Act*.[157] In evidence to the Senate Committee privacy inquiry, the Australian Government Attorney-General's Department noted that the small business exemption was of concern to the European Commission and that it is probably the key outstanding issue between the EU and Australia.[158]

---

152 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 11–12.

153 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 3.

154 European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (2000), 7.

155 *Privacy Amendment Act 2004* (Cth).

156 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

157 Ibid, 74.

158 Commonwealth of Australia, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 63 (C Minihan). This was confirmed more recently in a consultation with the Chair of the Article 29 Working Party: P Schaar, *Consultation OSC 1*, London, 1 November 2006. The small business exemption is discussed further in Ch 35.

28.134 There is no equivalent in the EU Directive to the *Privacy Act* exemption for small businesses. The Senate Committee privacy inquiry questioned the need to retain the small business exemption, in part because it is preventing recognition of Australian privacy laws under the EU Directive.[159]

28.135 In evidence to the Senate Committee privacy inquiry, the Law Institute of Victoria stated:

> If we do not comply with the EU directive, Australian businesses are going to be impacted in terms of the extent to which they can work offshore and deal with other jurisdictions.[160]

28.136 This view was not shared by all stakeholders making submissions to the Senate Committee privacy inquiry. For example, the Australian Direct Marketing Association (ADMA) submitted that organisations had not been hindered in their ability to conduct business with EU business partners. Similarly, the OPC stated that, in practice, businesses simply included the relevant privacy standards in contracts.[161]

28.137 The OPC Review suggested that the fact that Australian privacy law has not been recognised as adequate by the EU has not inhibited trade. It stated that 'only a very small proportion of the submissions received from stakeholders and few of the comments made in consultation meetings indicate that the failure to achieve EU adequacy has impaired business and trade with European organisations'.[162]

28.138 Nevertheless, the Senate Committee privacy inquiry also considered it desirable for Australia's privacy laws to gain formal recognition as being adequate. The Senate Committee recommended that:

> The review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, examine measures that could be taken to assist recognition of Australia's privacy laws under the European Union Data Protection Directive.[163]

28.139 The EU and Australia are engaged in ongoing negotiations on the issue of the adequacy of Australia's privacy regime for the purpose of the EU Directive.

---

159 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32]–[7.34], rec 12.

160 Ibid, [4.127].

161 Ibid, [4.130]. See also A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

162 The Review concluded, however, that although there was no evidence of a push from business for the EU's recognition of adequacy, there may be long term benefits for Australia to continue to work towards this aim. The Review also supported continuing work within APEC to implement the APEC Privacy Framework (discussed below): Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 75.

163 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 16.

The use of contracts for compliance with the EU Directive

28.140 Alongside legislation and self-regulatory arrangements, contracts have been recognised as a mechanism for enhancing privacy protection.[164] Article 26(2) of the EU Directive explicitly recognises that contracts may be one method of ensuring that personal data transferred from one country to another receive 'adequate protection'. A contract that would meet these criteria would have to bind the organisation receiving the data to meet the EU standards of information practices, such as the right to notice, consent, access and legal remedies.[165]

28.141 The OECD has identified the following as core elements of privacy protections that should be reflected in contractual provisions:

- substantive rules based on the principles in the OECD Guidelines, either by inclusion of the substantive rules in the contract or by reference to relevant laws, principles or guidelines;
- a means of ensuring accountability and verifying that the parties are complying with their privacy obligations;
- a complaints and investigations process, in the event that there is a breach of the privacy obligations; and
- a dispute resolution mechanism for affected parties.[166]

28.142 The Australian Bankers' Association and ADMA submitted to the OPC Review that it would be beneficial for standard contracts to be made readily available to organisations to assist them in transfering data to or from the EU or APEC regions.[167]

Is 'adequacy' necessary or desirable?

28.143 In IP 31, the ALRC asked whether adequacy of the *Privacy Act* under the EU Directive is necessary for the effective conduct of business with EU members, and desirable for the effective protection of personal information transferred into and out of Australia.[168]

---

164 Organisation for Economic Co-operation and Development, *Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks* (2000), 7.

165 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), 361.

166 Organisation for Economic Co-operation and Development, *Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks* (2000), 13.

167 Australian Bankers' Association, *Submission to Review of the Private Sector Provisions of the Privacy Act*, 22 December 2004; Australian Direct Marketing Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

168 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–5.

28.144 The ALRC noted that it was interested in what further measures are necessary to ensure the adequacy of Australia's privacy regime under the EU Directive, including whether the removal or amendment of the small business exemption and the employee records exemption would be desirable in this context. The ALRC also asked whether the availability of standard contractual clauses would be sufficient to meet the needs of Australian businesses in this regard.[169]

28.145 While some submissions noted that businesses seem to be able to carry out business internationally without Australia receiving an adequacy assessment,[170] others noted that, without an adequacy assessment, Australian organisations may be less competitive in the global market.[171] It also was submitted that it is desirable for Australian law at least to meet the EU standard of best practice,[172] and that adequacy for the purpose of the EU Directive has important symbolic significance, indicating that Australia takes privacy regulation seriously and seeks to promote best practice in this area.[173] The OVPC noted that the EU assessment of Australia's privacy laws is not limited to the federal regime but extends to each state and territory jurisdiction.[174]

28.146 The OPC submitted that, while adequacy is desirable in order to streamline trade, even in EU jurisdictions privacy protections may not always be implemented satisfactorily. The European Commission's *First Report on the Implementation of the Data Protection Directive* indicates that different jurisdictions have implemented the EU Directive in different ways and, as a result, unauthorised and possibly illegal transfers are being made to destinations, or recipients are not being guaranteed adequate protection.[175]

28.147 It was highlighted in one submission that there are a number of differences between NPP 9 and the EU Directive. For example, under NPP 9: consent for transfer does not have to be 'unambiguous'; organisations are allowed to make their own assessment of whether there is 'adequate protection' in the destination country; and the 'reasonable steps' test is much weaker than the nearest equivalent in art 26(2), in that it addresses only standards and not safeguards and the exercise of rights. It was also noted that there is no equivalent in NPP 9 to the public interest, legal claims, or vital interests derogations in art 26; and that NPP 9 does not provide any protection where

169 Ibid, [13.72].

170 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

171 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

172 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

173 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

174 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

175 Commission of the European Communities, *Report from the Commission: First Report on the Implementation of the Data Protection Directive*, 95/46/EC (2003), 19.

personal information is transferred to a state or territory government that is not subject to a privacy law.[176]

ALRC's view

28.148 The ALRC has been advised that the EU Directive can create problems for organisations that conduct business in Europe. It has been noted that the registration system in Europe is expensive, and that adequacy under the EU Directive nevertheless may still mean that organisations will be subject to additional requirements under privacy laws of individual European countries. The ALRC also notes that the European Commission's *First Report on the Implementation of the Data Protection Directive* found that the EU Directive has not guaranteed consistent privacy protection across Europe.[177]

28.149 The consensus view of submissions to this Inquiry suggests, however, that while a failure to achieve adequacy under the EU Directive is not preventing organisations from carrying out business internationally, an adequacy rating would help streamline trade between Australian businesses and Europe. The ALRC notes that the Australian Government apparently takes this view as it is continuing to work with the EU on the issue of the adequacy of Australia's privacy laws.

28.150 The ALRC makes a number of proposals in this Discussion Paper which may assist an adequacy finding under the EU Directive, including the: removal of the small business exemption and the employee records exemption; clarification of the 'required or authorised by or under law' exception; and development and publication of a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed UPPs.

Asia-Pacific Economic Cooperation Privacy Framework

28.151 The APEC Privacy Framework was endorsed by APEC Ministers in November 2004. The APEC Privacy Framework contains nine privacy principles recognising 'the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region'.[178]

28.152 As with the EU Directive, the APEC Privacy Framework aims to promote electronic commerce by harmonising members' data protection laws and facilitating information flow throughout the Asia-Pacific region.[179] Unlike the EU Directive,

---

176 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

177 Commission of the European Communities, *Report from the Commission: First Report on the Implementation of the Data Protection Directive*, 95/46/EC (2003), 19.

178 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), foreword. The APEC Privacy Framework is also discussed in Ch 4.

179 Ibid, [5]–[6].

however, APEC members are not obliged to implement the APEC Privacy Framework in any particular way domestically.[180]

28.153 APEC commenced development of the APEC Privacy Framework in 2003, which largely is based on the OECD Principles. Australia played a key role in the development of the APEC Privacy Framework, leading the APEC working group in the drafting process.

28.154 As noted in Part D, the APEC principles are intended to apply to persons or organisations in both the public and private sectors who control the collection, holding, use, transfer or disclosure of personal information.[181] The principles cover: preventing harm; notice; collection limitation; use of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.[182] The principles are intended to encourage the development of appropriate information privacy protections by members.[183]

28.155 One key area in which the APEC Privacy Framework takes a different approach to the EU Directive is in transborder data flows. Consultants to APEC, Malcolm Crompton and Peter Ford, have said:

> It is no longer accurate to describe data as 'flowing' at all … instead of point to point transfers, information is now commonly distributed among a number of data centres and is accessible globally over the Internet or over private networks.[184]

28.156 While the EU Directive is concerned with border controls and whether personal data are moving to a jurisdiction that has adequate protection, the APEC Privacy Framework holds the organisation sending the data accountable. Once an organisation has collected personal information, it remains accountable for the protection of those data even if they change hands or move from one jurisdiction to another.[185]

28.157 Principle 9 of the APEC Privacy Framework states that a personal information controller

> should be accountable for complying with measures that give effect to the Principles. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.

---

180 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.

181 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].

182 See Ibid, [14]–[26].

183 Ibid, preamble.

184 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.

185 Ibid, 8.

28.158 Principle 9 is therefore similar to NPP 9 in that it also uses the term 'reasonable steps'. The reference to 'due diligence' may be perceived, however, as stronger than the requirement of 'reasonable belief' in NPP 9.

28.159 Given the vast differences between the member economies of APEC, the APEC Privacy Framework does not aspire to uniformity but strives to recognise cultural and other diversities within its membership.[186] The APEC Privacy Framework encourages cooperation between members on the regional enforcement of data protection norms and the development of agreements between nations for cooperative enforcement.[187] These cross-border arrangements may include mechanisms to:

- notify public authorities in other member states of investigations and assistance in investigations; and
- identify and prioritise cases for cooperation in severe cases of privacy infringement that may involve authorities in several countries.[188]

28.160 APEC members also have agreed to support the development and recognition of members' cross-border privacy rules (CBPRs) across the APEC region. The APEC Privacy Framework states that:

> Member Economies should endeavour to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.[189]

28.161 The First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework was held on 22–23 January 2007 in Canberra. Its focus was the development and use of CBPRs by business, and the development of a model for implementing CBPRs. The seminar concluded that a 'Choice of Approach' model supported by trustmarks would be the most appropriate model. The key feature of this model is that each economy chooses the entities and procedures that will be used within the economy to assess the compliance of an organisation's CBPRs with the APEC Privacy Framework.

28.162 Under the model, an organisation that wishes to be considered as having CBPRs that comply with the APEC Privacy Framework submits an application containing its self assessment to a 'designated review entity' (which could include a privacy regulator or a trustmark body). By a framework agreed between the relevant entities of the APEC economies, a process is established to publish a centralised,

---

186 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [5]–[6].
187 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor* 8, 8.
188 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [46].
189 Ibid, [48].

publicly available list of the organisations whose CBPRs are assessed by designated review entities as being in compliance with the APEC Privacy Framework. Under the agreed framework, a participating economy accepts the assessments made by the designated entity in another participating economy following the choice of approach to CBPRs in that economy. The agreed framework also provides for communication and information sharing between the designated entities in each economy to facilitate the resolution of disputes relating to consumer complaints on cross-border handling of personal information.

28.163 Discussion at this meeting emphasised that trust marks could play a significant role in a CBPR system to assist economies in reviewing and giving recognition to organisations' CBPRs. A trustmark is a label or visual representation showing participation in a trustmark scheme in which a third party guarantees to consumers an organisation's compliance with the requirements for participation in that scheme. Trustmarks can be used to demonstrate compliance with a host of different principles, including privacy principles.[190]

28.164 The Second Technical Assistance Seminar on International Implementation of the APEC Privacy Framework was held in Cairns on 25–26 June 2007. It looked at developing and refining aspects of the 'Choice of Approach' model, by considering the cross-border cooperation arrangements between various stakeholders, which will be a necessary part of a CBPR system, and the steps economies can begin taking to implement parts of the preferred implementation model. The development of a 'Pathfinder' (or pilot project), which would involve a number of economies participating in a trial of a CBPR system was discussed at the seminar.

28.165 As noted above, Australia has been instrumental in the development of the APEC Privacy Framework. In the final report of the OPC Review, the OPC was supportive of the APEC Privacy Framework and expressed the view that:

> The initiative has the potential to accelerate the development of information privacy schemes in the APEC region and to assist in the harmonisation of standards across national jurisdictions.[191]

28.166 There has been some criticism that the APEC Privacy Framework is too 'light touch' in its approach and does not provide sufficient privacy protection for individuals. Greenleaf argues that the APEC Privacy Framework has a bias towards the free flow of personal information and does not recognise that there can be legitimate privacy reasons for restricting data exports.[192] The requirement either of consent or that the discloser takes reasonable steps to protect the information is said to be 'a very soft

---

190 Trustmarks are discussed further below.

191 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 75.

192 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 122.

substitute for a Data Export Limitation principle' along the lines of that contained in the EU Directive.[193]

28.167 Greenleaf has also noted that, although the APEC Privacy Framework does not set any requirements of its own, it does not prevent its members having their own data export restriction rules. Such rules could be for domestic purposes or to meet the requirements of the EU Directive.[194]

Asia-Pacific Privacy Charter Initiative

28.168 The Asia-Pacific Privacy Charter Council, a regional non-government expert group, has developed independent privacy standards for privacy protection in the Asia-Pacific region.[195] The Council has drafted the Asia-Pacific Privacy Charter (APP Charter) with the aim of influencing the development of privacy laws in the region in accordance with the standards set out in the Charter.[196]

28.169 The APEC Privacy Framework and the APP Charter have a number of similarities, and both reflect many of the principles contained in other international and regional agreements, such as the OECD Guidelines and the EU Directive.[197] The APP Charter, as it stands, however, is intended to be a 'maximalist' or 'high watermark' draft, reflecting all the significant privacy principles from relevant international instruments.[198]

28.170 The APEC Privacy Framework does not have a principle that explicitly limits data flows to countries without similar privacy laws. In contrast, Principle 12 of the APP Charter contains a limitation similar to that under the EU Directive. Principle 12 states that an organisation must not transfer personal information to a place outside the jurisdiction in which it is located unless:

- there is in force in that jurisdiction a law embodying principles substantially similar to the APP Charter Principles;
- it is with the consent of the person concerned; or

193 Ibid, 125.

194 G Greenleaf, 'APEC Privacy Framework Completed: No Threat to Privacy Standards' (2006) 11 *Privacy Law & Policy Reporter* 220.

195 Cyberspace Law and Policy Centre, 'Announcement: Asia-Pacific Privacy Charter Initiative' (Press Release, 1 May 2003). As at 31 July 2007, a second draft of the Charter had not yet been released for public comment.

196 See Ibid. The Charter is also discussed in Ch 4.

197 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, 1.

198 Ibid, 1.

- the organisation has taken all reasonable steps to ensure that the personal information will be dealt with in accordance with the APP Charter Principles in that place and continues to be liable for any breaches of the Principles.

28.171 This model is stronger than NPP 9(a) in that it does not allow an organisation merely to have a 'reasonable belief' that the recipient is subject to similar laws. The APP Charter also places the responsibility on the organisation to take reasonable steps *before* the personal information is transferred—not after, as is the case in NPP 9(f). The inclusion of the statement that the organisation must continue to be liable for any breaches of the Principles is in keeping with the APEC Privacy Framework, whereby the transferor of the information remains accountable for ensuring compliance with privacy measures.

Submissions and consultations

28.172 In IP 31, the ALRC asked whether the APEC Privacy Framework, or other standards, such as the APP Charter, provide an appropriate model for the protection of personal information transferred between countries.[199]

28.173 A number of stakeholders supported the APEC Privacy Framework.[200] For example, the OPC submitted that it provides a positive step forward in addressing regional consistency regarding the handling of personal information. Specifically, the Framework may function as a starting point to assist member economies that currently do not have any privacy regime to develop privacy protections for individuals' personal information.[201]

28.174 Microsoft Australia submitted that it prefers the APEC Privacy Framework approach to transborder data flows to the regime set out in NPP 9.

> The free flow of data across national borders is now a prerequisite to global commerce and unnecessary impediments to those flows should be removed wherever possible … Microsoft also observes that it is not only business practice that is accelerating the movement of information flows between economies. Technology is also a significant contributor and importantly, a significant contributor to it being undertaken in a way that respects privacy policies and choices. For this reason, privacy law that focuses on outcomes not process will help reduce the inevitable procedural inconsistencies between the regulation of privacy in different countries but also facilitate the accelerated development of technologically based privacy protection rather than hinder it.[202]

---

199 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 13–6.

200 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; ANZ, *Consultation PC 82*; Melbourne, 7 February 2007; Australian Compliance Institute, *Consultation PC 53*, Sydney, 17 January 2007.

201 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

202 Microsoft Australia, *Submission PR 113,* 15 January 2007.

28.175 The National Australia Bank and MLC submitted that the APEC Privacy Framework is an excellent start for the facilitation of information flows, but noted that it is only relevant to information flows between countries that are members of APEC.[203] There will still need to be models and frameworks, based on the requirements of NPP 9, which enable the flow of information to countries outside of APEC or any other member nation of differing charters or agreements.[204]

28.176 It was submitted, however, that the APEC Privacy Framework provides only a bare minimum of privacy protection and is aimed at those jurisdictions without an existing higher level.[205] Professor Greenleaf, Waters and Associate Professor Bygrave noted that the APEC Privacy Framework does not: forbid the transfer of personal information to countries without APEC-compliant laws; explicitly allow restrictions on transfer to countries without APEC-compliant laws; or allow transfers to countries that have APEC-compliant laws. It was also noted that the APEC Privacy Framework does not hold the data exporter 'accountable' in any meaningful sense, because it does not have any requirement of legal enforcement, and there is no guarantee of any legal remedy against the exporter, or the importer if it is in a jurisdiction without applicable privacy laws.[206] Some submissions noted that the APP Charter provides a more appropriate model for protecting privacy.[207]

ALRC's view

28.177 The APEC Privacy Framework is a significant development in addressing regional consistency in the handling of personal information. The ALRC notes that, in implementing the APEC Privacy Framework

> the means of giving effect to the Framework may differ between Member Economies, and it may be appropriate for individual economies to determine that different APEC Privacy Principles may call for different means of implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatibility of approaches in privacy protections in the APEC region that is respectful of requirements of individual economies.[208]

28.178 The involvement of Australia in the implementation of the APEC Privacy Framework will not require the lowering of any privacy protections under the *Privacy Act*. It may, however, provide new ways of encouraging compliance with local and international privacy standards. The ALRC notes that the Australian Government continues to play a key role in the implementation of the APEC Privacy Framework. The ALRC has borrowed elements from both the APEC Privacy Framework and the

---

203 India, for example, is not a member.
204 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.
205 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
206 G Greenleaf and N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
207 Ibid; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
208 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), 31.

APP Charter, as well as the NPPs and the EU Directive, in developing the proposed UPPs.[209]

Trustmarks

28.179 One feature of the APEC Privacy Framework that may have application in the Australian context is a trustmark scheme.[210] A number of countries already have adopted trustmark schemes, including privacy trustmark schemes. Some of these schemes are beginning to recognise each others' trustmarks and develop global trustmark principles.[211] Trustmark schemes vary in nature and structure. For example, in the US, trustmark bodies are private sector organisations,[212] whereas in Singapore, the National Trust Council's TrustSg is publicly supported by Singapore's Infocomm Development Authority.[213]

28.180 Trustmark bodies not only provide accreditation and allow the use of trustmarks, they also can provide advice to organisations and consumers about privacy laws and handle privacy complaints.[214] One advantage of adopting a trustmark scheme is that it can deal with low level privacy breaches and the provision of advice on privacy matters, leaving government regulators and law enforcement bodies to focus on serious and harmful privacy breaches.

28.181 One option would be the introduction of an Australian privacy trustmark scheme. An Australian privacy trustmark scheme could approve privacy policies for the purpose of the proposed 'Openness' principle in the UPPs. On approval an agency or organisation would be permitted to display a privacy trustmark. If an agency or organisation breaches an individual's privacy, a privacy trustmark body could provide an external dispute resolution scheme and could refer appropriate matters to the OPC. One enforcement option would be to prevent an agency or organisation displaying a trustmark. Once established, an Australian trustmark scheme could seek recognition by overseas trustmark schemes, and could be used to approve CBPRs for the purposes of the APEC Privacy Framework or other international privacy regimes.

28.182 Submissions from stakeholders did not raise the issue of trustmarks. The ALRC is interested in hearing views on the use of trustmarks to encourage compliance

---

209 See, eg, Proposal 28–4 above.

210 The ALRC notes that EU is currently considering the use of 'trust seals' in the context of privacy enhancing technologies. See Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* (2007), 228.

211 Examples include the BBB*Online* Japanese Privacy Seal: see BBBOnline, *BBBOnline Japanese Privacy Seal* <www.bbbonline.org/privacy/jipdec.asp> at 31 July 2007; the Asia Trustmark Alliance (ATA): TrustSg, *Asia Trustmark Alliance* <www.trustsg.com.sg/v3/for_merchants/ata.html> at 31 July 2007; and the Global Trustmark Alliance *Website*, <www.globaltrustmarkalliance.org> at 31 July 2007.

212 See, eg, TRUSTe, *Website* <www.truste.org>, at 31 July 2007.

213 TrustSg, *National Trust Council* <www.trustsg.com.sg/v3/for_merchants/ntc.html> at 31 July 2007.

214 See, eg, TRUSTe, *Website* <www.truste.org> at 31 July 2007.

with, and enforcement of, Australian and international privacy standards. Should they be provided for under the *Privacy Act*?

Question 28–2 Would the use of trustmarks be an effective method of promoting compliance with, and enforcement of, the *Privacy Act* and other international privacy regimes? If so, should they be provided for under the *Privacy Act*?

Summary of proposed 'Transborder Data Flows' principle

28.183 In summary, the eleventh principle in the proposed UPPs should be called 'Transborder Data Flows'. It should appear as follows:

UPP 11. Transborder Data Flows

An agency or organisation in Australia or an external Territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia only if:

(a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the UPPs; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

(vi) extradition and mutual assistance; or

(d) the agency of organisation continues to be liable for any breaches of the UPPs, and

(i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation;

(ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

(iv) all of the following apply: the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

(v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the UPPs.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

29. Additional Privacy Principles

Contents

Introduction 865
Accountability principle 866
Background 866
Submissions and consultations 868
ALRC's view 868
Prevention of harm principle 869
Background 869
Submissions and consultations 870
ALRC's view 871
No disadvantage principle 872
Background 872
Submissions and consultations 873
ALRC's view 873

Introduction

29.1 This chapter considers whether the *Privacy Act 1988* (Cth) should be amended to cover aspects of privacy that are not currently covered by the Information Privacy Principles (IPPs) or National Privacy Principles (NPPs).[1] Such new provisions could be located in the proposed Unified Privacy Principles (UPPs) or in other parts of the Act.

29.2 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether agencies and organisations should be subject to any additional privacy principles and, if so, what should be the content of these principles.[2] The following potential new privacy principles were identified: (a) an 'accountability' principle; (b) a 'prevention of harm' principle; (c) a 'consent' principle;[3] and (d) a 'data breach notification' principle[4]. During consultations, other new privacy principles were also suggested,

1 The ALRC proposes that the IPPs and NPPs should be consolidated into a single set of privacy principles, the UPPs, which would be generally applicable to agencies and organisations: see Proposal 15–2.

2 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 4–35.

3 The question whether there should be a separate privacy principle dealing with consent is addressed in Ch 16.

4 That is, the ALRC asked whether there should be a new privacy principle requiring an entity that holds personal information to notify any individual whose personal information has been, or is reasonably believed to have been, accessed without authorisation: Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–35 and 11–3(d). This issue is addressed in detail in Ch 47, where the

including a 'no disadvantage' principle. Some stakeholders supported the addition of one or more of these new privacy principles. Others, however, submitted simply that there should be no new privacy principles.[5]

29.3 This chapter considers whether the *Privacy Act* should impose requirements in relation to a number of the aspects of privacy listed above. If the answer to that threshold question is 'yes', the requirements could be implemented by:

- creating a new privacy principle to deal directly with the relevant aspect of privacy;
- amending the other, existing privacy principles to take account of the relevant aspect of privacy;
- locating the requirements elsewhere in the *Privacy Act*, or in a legislative instrument made pursuant to the Act, or in other sectoral legislation; or
- the Office of the Privacy Commissioner (OPC) or another entity issuing guidance to assist agencies and organisations to respond better to the relevant aspect of privacy.

Accountability principle

Background

29.4 Some have suggested that an 'accountability' privacy principle would be beneficial in establishing who is responsible for maintaining individuals' privacy rights. Such a provision exists in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines), which provides that 'a data controller should be accountable for complying with measures which give effect to the [other] principles [in the OECD Guidelines]'.[6]

29.5 Another example is provided in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which states:

> A personal information controller should be accountable for complying with measures that give effect to the Principles. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due

---

ALRC proposes an amendment to the *Privacy Act* to address data breach notification and explains why such a provision should not be located in the UPPs.

5 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

6 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 14.

> diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.[7]

29.6 The Asia-Pacific Privacy Charter Council (the APPC Council), a regional expert group, has developed independent privacy standards for privacy protection in the Asia-Pacific region. One of the principal tasks of the APPC Council is to draft the Asia-Pacific Privacy Charter (APP Charter).[8] The draft APP Charter, which includes general privacy principles that are intended to be observed by both the public and private sectors, provides that a regulated entity should be 'accountable for its compliance with these Principles and must ensure that an identifiable person is responsible for ensuring that the organisation complies with each Principle'.[9]

29.7 Some overseas jurisdictions have adopted an accountability principle in their privacy law. Part I of the *Federal Data Protection Act 1990* (Germany) (FDP Act), which applies to both the public and private sectors, directly implements the Accountability Principle in the OECD Guidelines. It requires the appointment of a data protection officer who is responsible for ensuring that the Act and other provisions concerning data protection are observed.[10]

29.8 Canadian privacy law, in some ways, goes further than this. The *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act) applies to private sector organisations in respect of personal information that they collect, use or disclose in the course of commercial activities or certain personal information about employees of organisations.[11] Subject to certain provisions, the PIPED Act requires organisations to comply with the National Standard of Canada *Model Code for the Protection of Personal Information*, which is a schedule to the Act.[12] It includes an accountability principle that states in part:

> An organisation … shall designate an individual or individuals who are accountable for the organisation's compliance with the [principles] …
>
> An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[13]

---

7 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 9.

8 See Cyberspace Law and Policy Centre, 'Announcement: Asia-Pacific Privacy Charter Initiative' (Press Release, 1 May 2003).

9 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, Principle 3.

10 *Federal Data Protection Act 1990* (Germany) ss 4f, 4g.

11 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(1).

12 Ibid s 5.

13 See Ibid sch 1, Principle 4.1.

29.9 The accountability principle also requires an organisation to implement policies and procedures to: protect personal information; establish procedures to respond to complaints and inquiries; train staff about the organisation's policies; and prepare information to explain the organisation's policies and procedures.[14]

Submissions and consultations

29.10 Some stakeholders supported the inclusion of a specific privacy principle dealing with accountability.[15] The National Association for Information Destruction submitted that such a principle should 'require businesses to take responsibility for certain types of information at the end of its cycle'.[16] The New South Wales Disability Discrimination Legal Centre proposed that such a principle should make organisations accountable for their compliance with the privacy principles and that an 'identifiable person' within an organisation should be responsible for ensuring that organisation's compliance.[17]

29.11 Other stakeholders specifically opposed the addition of an accountability privacy principle.[18] While noting that such a principle was theoretically beneficial, one submission questioned the practical utility of the current models of accountability principle:

> At first sight the addition of an express accountability principle would be welcome. But the existing models seem to add little of substance. The OECD accountability principle (14) is nothing more than a 'motherhood' statement, while the APEC Framework Accountability principle (IX) seems to be more to do with onward transfer obligations that are arguably best covered in security and transborder data principles, and also seems confused about the role of consent.[19]

29.12 AAMI noted that there are already accountability requirements that apply to organisations, particularly those in the financial services and insurance industries. It submitted that any accountability principle should follow these existing frameworks, and state how many days an organisation has to report a breach to the regulator.[20]

ALRC's view

29.13 The ALRC does not believe that the proposed UPPs should contain a discrete accountability principle. The ALRC holds this view for two main reasons. First, there are better mechanisms for establishing accountability, including the following:

---

14 Ibid sch 1, Principle 4.1.4.

15 National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

16 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

17 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

18 Australian Federal Police, *Submission PR 186,* 9 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

19 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

20 AAMI, *Submission PR 147,* 29 January 2007.

- the *Privacy Act* already establishes that where an agency or organisation is in breach of the privacy principles,[21] this constitutes an interference with privacy, which triggers the availability of a number of avenues to enforce compliance;[22]

- the ALRC proposes to establish a statutory cause of action that would provide a new method for individuals to make people accountable for breaches of privacy rights;[23] and

- a number of other privacy principles—especially those dealing with openness and specific notification—require agencies and organisations to make their practices for managing personal information transparent, thereby fostering accountability.[24]

29.14 Secondly, the ALRC agrees with the position, adopted in a number of submissions, that an accountability principle may be of limited practical utility. The main problems with establishing effective accountability arise where an agency or organisation subcontracts the handling of personal information to another entity, or where personal information is transferred outside Australia. The ALRC's view is that these specific problems should be dealt with in those contexts—for example, by consolidating the IPPs and NPPs, and tightening the rules in respect of personal information that is handled by contractors.[25] Similarly, as explained in Chapter 28, the ALRC proposes that the UPPs should contain a 'Transborder Data Flows' principle, applicable to agencies and organisations, which would ensure that data collectors are more accountable for the personal information that they collect and transfer.

Prevention of harm principle

Background

29.15 There is a question whether the UPPs should contain a 'prevention of harm' principle. Such a provision would require data collectors 'to prevent tangible harms to individuals and to provide for appropriate recovery for those harms if they occur'.[26] In other words, it would require data collectors to take a prophylactic approach, focusing on obviating potential problems before they are realised.

---

21 See *Privacy Act 1988* (Cth) ss 13, 13A. Currently, these provisions establish that a breach of the IPPs or NPPs is an interference with privacy. The ALRC's view is that a breach of the proposed UPPs should also be considered an interference with privacy.

22 Compliance and enforcement of the requirements in the privacy principles is discussed in Part F.

23 See Ch 5.

24 See, especially, Chs 20 and 21.

25 See, especially, Proposals 15–2 and 25–2.

26 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 28.

29.16 The APEC Privacy Framework contains such a principle. It states:

> Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.[27]

29.17 A provision of the German FDP Act, entitled 'Data avoidance and data economy', states:

> The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and psuedonymisation where possible and where the effort entailed is proportionate to the interests to be protected.[28]

Submissions and consultations

29.18 Some stakeholders supported the inclusion of a specific privacy principle dealing with prevention of harm.[29] Veda Advantage submitted that this aligns with the overall 'purpose of regulating information flows, [which] is to protect individuals from harmful uses of information'.[30]

29.19 A number of stakeholders opposed a prevention of harm principle.[31] One submission argued that this is an unsuitable subject to be addressed in a privacy principle.

> The sentiment that privacy remedies should concentrate on preventing harm … is unexceptional but it is strange to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other Principles makes it easier to justify exempting whole sectors (eg small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA).[32]

---

27 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), Principle 1.

28 *Federal Data Protection Act 1990* (Germany) s 3a.

29 Government of South Australia, *Submission PR 187,* 12 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

30 Veda Advantage, *Submission PR 163,* 31 January 2007.

31 Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; AAMI, *Submission PR 147,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

32 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007, citing G Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 91, 100.

29.20 The Law Council of Australia was concerned that such a principle would be too imprecise because it is difficult to discern a precise meaning of 'harm'.

> While financial harm and damage to reputation or character are concepts which are well understood, other concepts of harm which are raised within the privacy debate such as 'distress' and the knowledge that someone has their personal information are harder to place within a legislative context.[33]

29.21 While opposed to the addition of a prevention of harm principle, AAMI submitted that, if it were included, it should follow existing risk management frameworks.[34]

ALRC's view

29.22 The ALRC believes that the UPPs should not contain a discrete 'prevention of harm' principle. First, there does not appear to be a strong push among stakeholders to include such a principle. Indeed, the majority of stakeholders that commented on this issue were opposed to this reform.

29.23 Secondly, the ALRC believes that a number of the principles in the UPPs already incorporate a prevention of harm approach. In particular, the privacy principles dealing with data quality and data security impose specific obligations to ensure the integrity of personal information that is handled by agencies and organisations, and to guard against possible misuse and unauthorised disclosure.[35] Strengthening these provisions, as proposed by the ALRC, will reduce the risks associated with poor handling of personal information. Similarly, the proposed 'Anonymity and Pseudonymity' principle aims to reduce the threat of personal information being misused by directing agencies and organisations, where lawful and practicable, not to collect personal information in the first place.[36]

29.24 Thirdly, the ALRC is concerned that the obligations of a general prevention of harm principle will be undesirably vague. Professor Fred Cate has argued that privacy principles should 'target harmful uses of information, rather than mere possession'.[37] By concentrating on ways to prevent personal information being handled unfairly or otherwise inappropriately, this is precisely what the UPPs are intended to achieve.

---

33 Law Council of Australia, *Submission PR 177,* 8 February 2007.
34 AAMI, *Submission PR 147,* 29 January 2007.
35 Data quality and data security are discussed in Chs 24 and 25 respectively.
36 See Ch 17.
37 F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14, 28.

No disadvantage principle

Background

29.25 During the ALRC's submission and consultation process, it was suggested that consideration be given to the inclusion or incorporation of a 'no disadvantage' principle or provision. This would involve amending the *Privacy Act* to include a provision prohibiting agencies and organisations from unfairly disadvantaging an individual on the basis that he or she is seeking to assert or otherwise enjoy his or her privacy rights.

29.26 It may be argued, for instance, that an individual wishing to remain anonymous when transacting with an organisation should not be treated unfavourably because of this. Examples of unfavourable treatment may include the organisation charging a fee that would only apply to individuals who seek to transact anonymously, or withholding a product or service until the individual decides he or she no longer wishes to transact anonymously.

29.27 The *Privacy Act* does not currently contain an express, generally applicable 'no disadvantage' provision. There is no such provision in any other Australian jurisdiction. Nor is there such a provision in the OECD Guidelines or in the privacy legislation of the common law jurisdictions, such as the United Kingdom, Canada and the United States, with which Australia is most commonly compared. On the other hand, the draft APP Charter contains a 'non-discrimination' principle that states:

> People should not be denied goods or services or offered them on unreasonably disadvantageous terms (including higher cost) in order to enjoy the rights described in this Charter.
>
> The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.[38]

29.28 A similar provision is included in the Australian Privacy Charter.[39] The principle is said to be directed towards practices such as the following:

> Customers should not have to pay for the exercise of line-blocking or call-blocking facilities to prevent the display of the caller's telephone number. Similarly, this principle has application to customer loyalty schemes which allow organisations to develop extensive databases on a consumer's spending patterns by only allowing discounts if consumers identify themselves in transactions.[40]

---

38 G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources <www.worldlii.org/int/other/PrivLRes/2003/1.html> at 31 July 2007, Principle 5.

39 Australian Privacy Foundation, *Australian Privacy Charter* <www.privacy.org.au/About/PrivacyCharter.html> at 31 July 2007, Principle 18.

40 T Dixon, 'Privacy Charter Sets New Benchmark in Privacy Protection' (1995) 2 *Privacy Law and Policy Reporter* 41, 43.

29.29 While the *Privacy Act* does not currently contain a specific 'no disadvantage' provision, on one view, the NPPs already contain some provisions that are directed towards a similar policy goal. In particular, NPP 6.4 states:

> If an organisation charges for providing access to personal information, those charges:
>
> (a) must not be excessive; and
>
> (b) must not apply to lodging a request for access.

29.30 This provision aims to ensure that the access and correction rights provided for in NPP 6 are not undermined by organisations charging fees that make it prohibitively expensive to enjoy those rights. Similarly, a number of the NPPs require an organisation to take 'reasonable steps' to protect individuals' privacy rights.[41] Such a requirement is designed to promote substantive, rather than merely formal, enjoyment of privacy rights.

Submissions and consultations

29.31 Some stakeholders supported the addition of a no disadvantage principle.[42] The Australian Privacy Foundation submitted that this would 'ensure that data users do not use pricing or other sanctions to deter individuals from exercising their privacy rights'.[43] It was submitted that such a principle would offer additional protections to individuals beyond the pricing limitations included in some privacy principles.[44]

29.32 It was recognised, however, that a no disadvantage principle could hamper technological developments that involve data collection and it may not readily 'accommodate traditional privacy rights'. Consequently, 'such a principle would need to [be] designed carefully to avoid becoming a constraint on innovation'.[45]

ALRC's view

29.33 While supporting the general objective of a 'no disadvantage' principle—that individuals should not be unfairly disadvantaged by seeking to assert their privacy rights—the ALRC does not believe that a separate no disadvantage principle in the UPPs is the most appropriate vehicle to achieve this. Rather, the ALRC's view is that this requirement should be incorporated, where appropriate, into some of the other privacy principles and in guidance from the OPC.

---

41 See *Privacy Act 1988* (Cth) sch 3, NPPs 1.3, 1.5, 3, 4, 5.2.

42 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

43 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

44 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

45 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

29.34 Some privacy principles already include a 'no disadvantage' element. As noted above, NPP 6.4 prohibits an organisation from charging excessive fees in respect of access to, and correction of, personal information held by the organisation. The ALRC proposes to retain this provision in the proposed UPPs because it is a practical way in which individuals can be protected from being disadvantaged for asserting their rights under the *Privacy Act*.[46]

29.35 One important way in which the 'no disadvantage' objective can be incorporated into the operation of the privacy principles more generally is through careful interpretation of the requirement on agencies and organisations to take 'reasonable steps' to protect individuals' information privacy in particular respects. For example, the ALRC proposes that agencies and organisations should be required to take reasonable steps to destroy or render non-identifiable personal information that they no longer need.[47] The ALRC believes that this requirement should be interpreted to mean that costs associated with destroying or rendering the information non-identifiable should be treated as normal operating costs of the agency or organisation in question, and not a cost imposed on the individual involved.

29.36 The ALRC also proposes that if an individual requests access to an agency's or organisation's Privacy Policy, the proposed 'Openness' principle provides that the agency or organisation must take reasonable steps to make this available without charging the individual for it.[48]

29.37 Similarly, the proposed UPPs state that, wherever it is lawful and practicable, agencies and organisations must give individuals the clear option of transacting anonymously or pseudonymously.[49] The fact that this obligation only applies when *practicable* is a significant qualification. The ALRC believes, however, that this requirement cannot logically be interpreted as allowing agencies and organisations to put unreasonable impediments or disincentives in the way of individuals exercising this option. For example, it would not be reasonable for individuals to be charged a punitive fee for choosing to remain anonymous in their transactions with an agency or organisation.[50]

---

46 See Ch 26.

47 See Ch 25. Note also that a similar obligation already applies to organisations: *Privacy Act 1988* (Cth) sch 3, NPP 4.2.

48 See Ch 21.

49 See Ch 17.

50 An example of this arises, in the specific context of telecommunications, in relation to the practice of charging individuals who wish to obtain a 'silent' telephone number. See Proposal 63–11.

30. Overview—Exemptions from the *Privacy Act*

Contents

Introduction 877
Exemptions under the *Privacy Act* 878
Public sector exemptions 879
Private sector exemptions 880
Exemptions under international instruments 881
OECD Guidelines 881
EU Directive 882
APEC Privacy Framework 882
Should there be any exemptions from the *Privacy Act*? 883
Submissions and consultations 884
ALRC's view 886
The number and scope of exemptions 887
The number of exemptions 887
The scope of the exemptions 888
Submissions and consultations 890
ALRC's view 891
Complexity of the exemption provisions 892
Submissions and consultations 893
ALRC's view 894
Location of the exemption provisions 894
Submissions and consultations 895
ALRC's view 896

Introduction

30.1 The application of the *Privacy Act 1988* (Cth) is limited by a number of exemptions and exceptions. This Discussion Paper distinguishes between exemptions, partial exemptions and exceptions to the requirements set out in the *Privacy Act*.[1] An *exemption* applies where a specified entity or a class of entity is not required to comply with the privacy principles that would otherwise be applicable to it. For example, a

1 Compare B Stewart, 'The New Privacy Laws: Exemptions and Exceptions to Privacy' (Paper presented at The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

'small business operator' is exempt from the requirement to comply with the rules in the *Privacy Act*. A *partial exemption* applies where a specified entity or a class of entity is required to comply with either: (1) only some, but not all, of the privacy principles; or (2) some or all of the privacy principles, but only in relation to certain of its activities. For example, the federal courts are *partially exempt* as they are only required to comply with the *Privacy Act* in relation to their administrative activities. An *exception* applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. For example, there is an exception to the prohibition against an organisation using or disclosing personal information for a secondary purpose where the individual in question has given his or her consent.[2]

30.2 This chapter provides an overview of the exemption provisions under the *Privacy Act*, outlines the exemptions under international instruments and considers issues concerning the existing exemptions from the Act. The remaining chapters in Part E examine specific exemptions from the *Privacy Act* in the public and private sectors, and considers whether new exemptions should be added to the Act. Exceptions to the privacy principles are discussed in Part D.

Exemptions under the *Privacy Act*

30.3 There are a number of ways in which entities can be exempt, either completely or partially, from the *Privacy Act*. Entities may be exempt from the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs) (or an approved privacy code),[3] the tax file number provisions or the credit reporting provisions of the Act.

30.4 Broadly speaking, the IPPs apply to acts and practices of Australian Government agencies and the NPPs apply to acts and practices of private sector organisations.[4] Entities that fall within the definition of an 'agency' therefore will be bound by the IPPs, and those that fall within the definition of an 'organisation' will be bound by the NPPs.

30.5 Where entities fall within the definition of an 'agency' or an 'organisation', their acts and practices may still be exempt from the *Privacy Act* if those acts or practices are excluded from the definition of an 'act or practice' to which the Act applies. Under s 7 of the Act, a reference to an 'act or practice' is generally a reference to an act done, or a practice engaged in, by: an agency, a file number recipient, a credit reporting agency or a credit provider. The section, however, excludes a wide range of activities of certain specified entities. For example, while federal courts fall within the definition

---

2 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(b).

3 Where the Privacy Commissioner has approved a privacy code for a particular organisation or industry, it replaces the NPPs for those organisations that are bound by the code. To the extent that an organisation is not bound by such a code, it is bound by the NPPs: Ibid s 16A(2).

4 Ibid ss 16, 16A.

of an 'agency' under the Act, their acts and practices are only covered by the IPPs if they relate to administrative matters.[5] Any activity of the courts that relates to non-administrative matters falls outside the definition of 'act or practice' and, therefore, is exempt from the *Privacy Act*.

30.6 Part IIIA of the Act regulates the handling of credit information about individuals by credit reporting agencies and credit providers. Individuals and entities are exempt from the credit reporting provisions where they fall outside the definition of a 'credit reporting agency' or a 'credit provider', or where their acts and practices are excluded by s 7 of the Act. Credit reporting is discussed in Part G.

Public sector exemptions

30.7 The *Privacy Act* prohibits an agency from engaging in an act or practice that breaches the IPPs.[6] Agencies are not subject to the private sector provisions of the Act unless they have been prescribed by regulation.[7] An agency may also be subject to the tax file number provisions and the credit reporting provisions of the Act in some circumstances.[8]

30.8 Agencies include: Australian Government ministers and departments; bodies and tribunals established under Commonwealth and ACT laws; Australian Government statutory office holders and administrative appointees; federal courts; and the Australian Federal Police. The definition of agency excludes incorporated companies, societies and associations even if they are established under Commonwealth law.[9]

30.9 The definition of agency excludes an organisation within the meaning of the *Conciliation and Arbitration Act 1904* (Cth) (now repealed)[10] and a branch of such an organisation.[11] This refers to federally registrable employer and employee associations and federally registrable enterprise associations.[12] In Chapter 3, the ALRC proposes that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity.[13] Since the *Conciliation and Arbitration Act* has been repealed, this provision should be updated as part of the proposed amendment of the Act.

30.10 Any act or practice engaged in by, or information disclosed to, a person in the course of employment by or in the service of an agency is treated as having been done

---

5 Ibid ss 6(1), 7(1)(a)(ii), (b).
6 Ibid s 16.
7 Ibid ss 6C, 7A, 16A.
8 Ibid ss 11, 11A, 11B.
9 Ibid s 6(1).
10 The *Conciliation and Arbitration Act 1904* (Cth) was repealed by s 3 of the *Industrial Relations (Consequential Provisions) Act 1988* (Cth).
11 *Privacy Act 1988* (Cth) s 6(1).
12 *Workplace Relations Act 1996* (Cth) sch 2, cl 18.
13 Proposal 3–2.

by, engaged in by or disclosed to the agency.[14] A person is not, however, to be regarded as an agency merely because he or she is the holder of, or performs the duties of: a judge or magistrate; a member of a prescribed Commonwealth tribunal; a prescribed office under the *Privacy Act* or the *Freedom of Information Act 1982* (Cth) (FOI Act);[15] or an office established under a Commonwealth or ACT law for the purposes of an agency.[16]

30.11 Chapters 31–34 discuss agencies that are completely or partially exempt from the *Privacy Act*—namely, defence and intelligence agencies, federal courts and tribunals, agencies listed under the FOI Act— and other public sector exemptions.

Private sector exemptions

30.12 The NPPs bind entities that fall within the definition of an 'organisation'. An 'organisation' is defined as an individual, a body corporate,[17] a partnership,[18] any other unincorporated association[19] or a trust[20] that is not exempt from the operation of the *Privacy Act*.[21] Certain entities are specifically excluded from the definition of 'organisation' and are therefore exempt from the Act. These exempt entities include small business operators, registered political parties, agencies, state and territory authorities, and prescribed state and territory instrumentalities.[22]

30.13 Certain acts and practices of organisations are also exempt from the operation of the *Privacy Act*. There are four ways in which an act or practice may be exempted from the Act. An act or practice may be excluded from:

---

14 *Privacy Act 1988* (Cth) s 8.

15 No such offices have been prescribed under either Act.

16 *Privacy Act 1988* (Cth) s 6(5).

17 A body corporate is any entity that has a legal personality under Australian law or the law of another country: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 4.

18 Any act or practice engaged in by one of the partners in a partnership is deemed to be an act or practice of the organisation. Obligations under the *Privacy Act 1988* (Cth) are imposed on each partner but may be discharged by any of the partners: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 5.

19 An unincorporated association includes a cooperative. The *Privacy Act 1988* (Cth) also covers acts or practices engaged in by an individual in his or her capacity as a member of the cooperative's committee of management. The *Privacy Act* imposes obligations on each member of the committee of management but may be discharged by any of the members of that committee: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 5.

20 An act or practice engaged in by a trustee is taken to have been engaged in by the trust. Obligations under the *Privacy Act 1988* (Cth) are imposed on each trustee but may be discharged by any of the trustees: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 5.

21 *Privacy Act 1988* (Cth) s 6C.

22 Ibid s 6C.

- what constitutes a breach of the NPPs or an approved privacy code;
- what constitutes an interference with the privacy of an individual;
- the definition of an act or practice; or
- the operation of the Act.

30.14 Chapters 35–39 examine current exemptions from the *Privacy Act* that apply to organisations, including the small business exemption, the employee records exemption, the media exemption, the political exemption and other private sector exemptions. Chapter 40 considers whether new exemptions should be introduced.

Exemptions under international instruments

OECD Guidelines

30.15 The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines) do not refer to exemptions.[23] They do, however, provide expressly for the possibility of excluding personal data from the application of the Guidelines that 'obviously do not contain any risk to privacy and individual liberties'.[24]

30.16 In addition, the Guidelines recognise that there may be exceptions to the privacy principles. OECD Guideline 4 provides two general criteria to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public.[25] Acceptable bases for exceptions set out in the OECD Guidelines include national sovereignty, national security, public policy and the financial interests of the state.[26] Importantly, the OECD Guidelines state that exceptions should be limited to those that are necessary in a democratic society.[27]

30.17 The Memorandum to the OECD Guidelines acknowledges that opinions may vary on the question of exceptions. It recognises that member countries may apply the Guidelines differently to particular kinds of personal data or in particular contexts, for example, credit reporting, criminal investigation and banking.[28]

---

23 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).
24 Ibid, Guideline 3(b).
25 Ibid, Guideline 4.
26 Ibid; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), Guideline 4; Memorandum, [46].
27 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Memorandum, [47].
28 Ibid, Memorandum, [19(g)], [47].

30.18 The OECD Guidelines also recognise that the application of the Guidelines is subject to various constitutional limitations in federal countries and therefore there are no requirements to apply the Guidelines beyond the limits of constitutional competence.[29]

EU Directive

30.19 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains a number of specific exemptions from, and exceptions to, the principles.[30] Exemptions under the EU Directive include the processing of data by: a natural person in the course of a purely personal or household activity;[31] and political parties in compiling data on individuals' political opinions in the course of electoral activities.[32]

30.20 Examples of exceptions to the privacy principles in the EU Directive include processing of data: necessary for the prevention, investigation, detection and prosecution of criminal offences;[33] concerning public security, defence, state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in areas of criminal law;[34] and for journalistic purposes or the purpose of artistic or literary expression if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[35]

APEC Privacy Framework

30.21 Under the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, exceptions to privacy principles are to be 'limited and proportional to meeting the objectives to which the exceptions relate', and they are to be made known to the public or in accordance with law.[36]

30.22 The APEC Privacy Framework defines 'personal information controller' to exclude an individual who deals with personal information in connection with his or her personal, family or household affairs.[37] Like the EU Directive, the APEC Privacy Framework is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy

---

29 Ibid, Guideline 5; Memorandum, [48].
30 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).
31 Ibid, art 3(2).
32 Ibid, Recital 36.
33 Ibid, art 13(1)(d).
34 Ibid, art 3(2).
35 Ibid, art 9. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), Recitals 17, 37.
36 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].
37 Ibid, [10].

interests.[38] Unlike the EU Directive, the APEC Privacy Framework does not contain exceptions for journalistic, literary or artistic expression, or an exemption for political parties in respect of their political or electoral activities.

Should there be any exemptions from the *Privacy Act*?

30.23 Before examining whether the existing exemptions from the *Privacy Act* are appropriate, the threshold question is whether the Act should contain any exemptions at all. Roger Clarke has suggested that there should be no exemptions from the privacy principles. In his view, privacy principles should be universal statements that convey the idea that the principles are paramount. The manner in which they are formulated and applied in practice should involve careful balancing between privacy and other interests so that the principles are not infringed. He argues that powerful interests are protected through large numbers of vague and extensible exemptions, and that privacy protection is entirely lost once a class of organisation or activity is exempted from the privacy principles.[39]

30.24 Blair Stewart, of the Office of the Privacy Commissioner, New Zealand, has taken a different view.[40] He conceded that well-drafted exceptions to specific privacy principles are preferable to excluding an entire class of entities or information. Stewart argued, however, that some types of entities and information should be excluded from the coverage of privacy principles so that the principles remain 'workable, general and not overly complex'—for example, it might be better not to apply some principles to intelligence agencies than to have exceptions for national security throughout the principles.[41]

---

38 Ibid, [13].

39 R Clarke, *Exemptions from General Principles Versus Balanced Implementation of Universal Principles* (1998) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Except.html> at 31 July 2007.

40 B Stewart, 'The New Privacy Laws: Exemptions and Exceptions to Privacy' (Paper presented at The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century, Sydney, 19 February 1997).

41 Ibid, 10.

30.25 Privacy legislation in some overseas jurisdictions contains full or partial exemptions relating to, for example, personal information handled by: individuals for the purposes of their personal, family or household affairs;[42] intelligence agencies;[43] and news media in relation to journalism or news activities.[44]

Submissions and consultations

30.26 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether it is appropriate for certain entities to be exempt, either completely or partially, from the operation of the *Privacy Act*.[45] A number of stakeholders submitted that there should be few, if any, blanket exemptions from the *Privacy Act*.[46]

30.27 The Office of the Victoria Privacy Commissioner stated that:

> In principle, organisations should not be completely exempt from having to comply with privacy obligations. Instead, policy makers should identify what practices (eg judicial activities) or principles should be adjusted or exempted/excepted. Some principles should apply across all organisations, such as the obligations to take reasonable steps to secure data and make sure it is accurate, complete and up to date.
>
> The privacy legislation should only be subject to such reasonable limits, to take up the wording in the Victorian Charter of Human Rights and Responsibilities Act 2006, as can be demonstrably justified in a free and democratic society.[47]

30.28 It was suggested in one submission that 'the exemptions and exceptions lead to an inequitable situation where privacy rights afforded depend on who is being dealt with'.[48] Another view was that 'if government agencies are allowed exemptions the Privacy Act as a whole is weakened'.[49]

30.29 It was also submitted that the only exemptions that are justifiable are exemptions for individuals handling personal information solely for non-business purposes, or entities that are subject to equivalent privacy laws—such as state and

---

42 See, eg, *Data Protection Act 1998* (UK) s 36; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2)(b); *Personal Data Act 1998* (Sweden) s 6; *Privacy Act 1993* (NZ) s 56; *Data Protection Act 1988* (Ireland) s 1(4)(c); *Personal Data (Privacy) Ordinance* (Hong Kong) s 52.

43 See, eg, *Privacy Act 1974* 5 USC § 552a (US) (j)(1); *Privacy Act 1993* (NZ) s 57. See also *Personal Data (Privacy) Ordinance* (Hong Kong) s 57 (exemption of personal data held by or on behalf of the government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong).

44 See, eg, *Privacy Act 1993* (NZ) s 2(1) (definition of 'agency'); *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

45 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–1.

46 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; SBS, *Submission PR 112,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

47 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

48 I Turnbull, *Submission PR 82,* 12 January 2007.

49 K Handscombe, *Submission PR 89,* 15 January 2007.

territory authorities.[50] Several stakeholders expressed support for exempting defence and intelligence agencies from the *Privacy Act*.[51]

30.30 In contrast, a few stakeholders specifically stated that it is appropriate to have exemptions from the *Privacy Act*.[52] While both the Australian Broadcasting Corporation (ABC) and SBS submitted that there should be few blanket exemptions from the *Privacy Act*, they suggested that the EU Directive and other international instruments illustrate a number of clear policy reasons why certain exemptions should be maintained. The ABC submitted that many, if not all, of the exemptions under the Act are based on similar policy concerns to those reflected in international instruments.[53] SBS stated that the justification for exemptions that are common to all international instruments is the need to balance privacy rights against a public interest purpose, such as matters essential to law and governance and freedom of expression.[54]

30.31 The ABC and SBS also submitted that, in the interest of certainty, exemptions are preferable to exceptions to specific privacy principles.[55] The ABC stated that:

> It should be recognised that while some blanket exemptions for whole classes of agencies and organisations may be described as undesirable and a blunt instrument for dealing with the potential for overreach in the operation of privacy principles … other more targeted exemptions, such as exemptions for specified acts or operations, can reflect a careful balancing of privacy and other interests.[56]

30.32 SBS suggested that a universal statement of principles would be unworkable, as it would result in uncertainty and extensive litigation before the application of the principles could be understood.[57]

30.33 The Real Estate Institute of Australia took the view that:

> To subject all entities to overly rigorous privacy protection without regard for relative risk or particular circumstance would simply result in an unnecessary and disproportionate compliance burden which would be passed on to consumers in terms of increased prices for affected goods and services. Further, it is likely that there would be some instances where the imposition of privacy requirements may impinge

---

50 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

51 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007.

52 SBS, *Submission PR 112,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

53 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

54 SBS, *Submission PR 112,* 15 January 2007.

55 Ibid; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

56 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

57 SBS, *Submission PR 112,* 15 January 2007.

> on the ability of certain persons, organizations or agencies to carry out activities which are in the national interest.[58]

30.34 The Fundraising Institute–Australia Ltd expressed a contrary view, submitting that the exemption for commercial entities, such as small businesses, undermines public confidence that the *Privacy Act* will adequately protect personal information.[59]

ALRC's view

30.35 Privacy interests in some cases may be outweighed by other public interests, such as national security, the administration of justice and the free flow of information to the public by the media. The purpose of having exemption provisions is to balance the need to protect privacy against these other interests. The need for balance between these different interests is reflected in international instruments.

30.36 The ALRC acknowledges that a blanket exemption from privacy legislation can be a blunt instrument, in that it exempts all activities of a specified entity or class of entities, regardless of whether the particular activity relates to the conflicting public interest. There are some entities, such as defence and intelligence agencies, however, whose principal function is in direct conflict with a number of the privacy principles. Other entities, such as royal commissions, inquire into matters of public interest and, therefore, should have their own information-handling standards tailored to their special role. Courts have an adjudicative function that also requires special rules regarding information handling, in order to balance privacy interests with the principle of open justice. In all three examples, exemptions from the *Privacy Act* are appropriate provided that there are other information-handling standards, such as ministerial privacy guidelines, that apply to the exempted entity.

30.37 In addition, entities that are subject to obligations that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act*, should be exempt from the Act—as the need to comply with two equivalent regimes would unnecessarily add to the compliance burden for such entities. Accordingly, in Chapter 34, the ALRC proposes that, before states and territories enact legislation applying the proposed Unified Privacy Principles and the proposed *Privacy (Health Information) Regulations*, the Act be amended to apply to state and territory incorporated bodies—except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act*.[60]

---

58 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
59 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.
60 Proposal 34–3.

The number and scope of exemptions

The number of exemptions

30.38 The *Privacy Act* has been criticised for the large number of exemptions it contains.[61] In the public sector, there are three classes of agencies—federal courts, ministers and royal commissions—and more than 20 specific, named agencies that are partially or completely exempt from the Act. In the private sector, in addition to the four exempt classes of entities—namely, small business operators, registered political parties, state and territory authorities, and prescribed state and territory instrumentalities—there are eight categories of organisations that are exempt from the Act.[62]

30.39 The OECD Guidelines state that there should be 'as few as possible' exceptions to the privacy principles.[63] Similarly, under the APEC Privacy Framework, exceptions to the principles are to be 'limited and proportional to meeting the objectives to which the exceptions relate'.[64]

30.40 One commentator has expressed the view that keeping exemptions to a minimum, and limiting them to particular provisions of the law whenever possible, are important to ensure that privacy protection applies as widely as possible throughout the community.[65] Another commentator argues that the effect of the large number of private sector exemptions in the *Privacy Act* is to legitimise the data processing practices of certain organisations, thus failing adequately to protect the privacy of individuals.[66]

30.41 Privacy legislation in some jurisdictions contains significantly fewer exemptions than the *Privacy Act*. For example, there are four exemptions in the United Kingdom,[67]

---

61 R Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (1989) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html> at 30 July 2007; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000.

62 *Privacy Act 1988* (Cth) ss 7B(1) (individuals acting in non-business capacity), (2) (contracted service provider for a Commonwealth contract), (3) (current or former employers of an individual), (4) (media organisations), (5) (contracted service providers for a state contract); 7C (political representatives); 13B (related bodies corporate); 13C (partnerships).

63 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4(a).

64 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

65 N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168.

66 H Lloyd, 'Are Privacy Laws More Concerned with Legitimising the Data Processing Practices of Organisations than with Safeguarding the Privacy of Individuals?' (2002) 9 *Privacy Law & Policy Reporter* 81.

67 *Data Protection Act 1998* (UK) ss 30(2) (personal data in respect of which the data controller is a proprietor of, or a teacher at, a school, or education authority in Scotland), 30(3) (personal data processed by government departments, local authorities, voluntary organisations or other bodies in the context of carrying out social work), 31 (personal data processed for the purposes of discharging functions relating

15 in New Zealand[68] and three in Hong Kong.[69] Although there are some exemptions common to both Australia and comparable jurisdictions—such as exemptions relating to personal use, national security, defence and journalism—a number of exemptions from the *Privacy Act* are not provided for in other jurisdictions. For example, unlike the *Privacy Act*, legislation in the United Kingdom, Canada and Hong Kong does not contain exemptions for specified government bodies such as defence agencies and Auditors-General.[70] In the United Kingdom, Canada and New Zealand, there is no exemption that applies to small businesses, employee records, registered political parties, or political acts and practices.[71]

The scope of the exemptions

30.42 In relation to the public sector, the acts and practices of some agencies—namely, the Australian Crime Commission, royal commissions and the intelligence agencies—are completely exempt from the *Privacy Act*.[72] The intelligence agencies are defined as the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Office of National Assessments (ONA).[73]

30.43 In relation to the private sector, certain entities are specifically excluded from the definition of 'organisation' and therefore are exempt from compliance with the NPPs, unless they fall within one of the conditions under which the exemption does not apply. These entities include small business operators, registered political parties, state

---

to regulatory activity), 36 (personal data processed by individuals for domestic purposes). Note that although Schedule 7 to the Act is entitled 'Miscellaneous Exemptions', the provisions in that schedule are exceptions to specific data protection principles, rather than exemptions.

68 *Privacy Act 1993* (NZ) ss 2(1) (the term 'agency' does not include: the Sovereign; the Governor-General or the Administrator of the Government; the House of Representatives; a member of Parliament in his or her official capacity; the Parliamentary Service Commission; the Parliamentary Service (with certain exceptions); in relation to its judicial functions, a court; in relation to its judicial functions, a tribunal; an Ombudsman; a royal commission; a commission of inquiry appointed under the *Commissions of Inquiry Act 1908* (NZ); a commission, board, court or committee of inquiry appointed by statute to inquire into a specified matter; or in relation to its news activities, any news medium), 56 (personal information held by individuals for the purposes of their personal, family, or household affairs), 57 (information held by intelligence organisations).

69 *Personal Data (Privacy) Ordinance* (Hong Kong) ss 52 (personal data held by individuals for the purposes of their personal, family or household affairs), 57 (personal data held by or on behalf of the government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong), 61 (personal data held by a data user whose business consists of a news activity and solely for the purpose of that activity). Note that although Part VIII of the Ordnance is entitled 'Exemptions', some of the provisions in that part are exceptions to the data protection principles, rather than exemptions: see, eg, *Personal Data (Privacy) Ordinance* (Hong Kong) ss 53 (employment—staff planning), 60 (legal professional privilege), 62 (statistics and research).

70 *Data Protection Act 1998* (UK); *Privacy Act* RS 1985, c P-21 (Canada); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Personal Data (Privacy) Ordinance* (Hong Kong).

71 *Data Protection Act 1998* (UK); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Privacy Act 1993* (NZ).

72 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (iv), (v), (2)(a), (c). The acts and practices of the Integrity Commissioner will also be exempt from the *Privacy Act* upon commencement of the *Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006* (Cth) sch 1, item 50.

73 *Privacy Act 1988* (Cth) s 6(1).

and territory authorities, and prescribed state and territory instrumentalities.[74] As a result, a large number of entities are exempt from the *Privacy Act*. The Australian Government Department of Employment, Workplace Relations and Small Business has estimated that approximately 94% of businesses may be exempt from the private sector provisions of the Act.[75]

30.44 Professor Graham Greenleaf and Nigel Waters have suggested that blanket exemptions for whole classes of agencies and organisations are undesirable.[76] Roger Clarke has argued that any form of exemption is a very blunt instrument because 'it creates a void within which uncontrolled abuses can occur'.[77]

30.45 It has also been suggested that some of the exemption provisions are expressed too broadly.[78] For example, acts and practices of a media organisation done 'in the course of journalism' are exempt from the Act.[79] A 'media organisation' is an organisation that collects, prepares or disseminates materials having the character of news, current affairs, information or documentaries to the public; or commentary or opinion on, or analysis of, these materials.[80] The terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' are not defined. One commentator has argued that the lack of definitions and the inclusion of 'information' separately from news, current affairs and documentaries allow any organisation aiming to publish material to take advantage of the exemption.[81]

---

74 Ibid s 6C(1).

75 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.20].

76 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 1; N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168.

77 R Clarke, *Flaws in the Glass; Gashes in the Fabric* (1997) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Flaws.html> at 31 July 2007.

78 See, eg, T Dixon, *Government Tables New Privacy Legislation* (2000) AustLII <www.austlii.edu.au/au/other/CyberLRes/2000/6/> at 31 July 2007; Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000.

79 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

80 Ibid s 6(1).

81 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.

Submissions and consultations

The number of exemptions

30.46 Several stakeholders expressed concern that there are too many exemptions from the *Privacy Act*.[82] The Office of the Privacy Commissioner (OPC) submitted that exemptions under the *Privacy Act* should be minimised in order to achieve uniformity and consistency of application of privacy legislation, and that a clear public interest for the exemptions should exist to support their creation or continuation. The OPC suggested that 'existing exemptions contained in the *Privacy Act* have developed over time and in some instances may require review to assess their continuing suitability'.[83]

30.47 The Centre for Law and Genetics also considered the substantial number of exemptions as a matter of concern.

> This growth of exemptions, if unchecked, has the potential to undermine the operation of the principles contained in the legislation and compromise the privacy rights of individuals.[84]

30.48 Similarly, the Legal Aid Commission of New South Wales submitted that 'the Act would be more effective if there were fewer exemptions, but a more flexible approach to applying the principles to different circumstances'.[85]

The scope of the exemptions

30.49 A number of stakeholders suggested that exemptions should be justified and limited to the extent possible[86] and emphasised the need for a clear rationale for each exemption.[87]

30.50 The Social Security Appeals Tribunal stated that 'agencies should not be excluded from the operation of the *Privacy Act* by genus'.[88] By contrast, the OPC emphasised the need to ensure the consistent coverage of entities that have a similar nature and function:

> A review of exemptions to the Privacy Act should also address irregularity of exemption coverage; that is where a specific entity is exempted from coverage of the Privacy Act while other entities of a similar nature and function are not. An example of this might be the coverage of tribunals by the Privacy Act, some of which are

---

82 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

83 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

84 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

85 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

86 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

87 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

88 Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

> covered by the Act and others of which are partially exempted. The Office believes consistent application of exemptions will foster greater clarity as to the intentions and coverage of exemptions.[89]

30.51 Some stakeholders submitted that it is preferable for exemptions to be targeted at either: specified acts and practices;[90] particular types of information; or specific information handling purposes.[91] One submission suggested that entities should apply for exemption from the *Privacy Act* on a case-by-case basis, and that any exemption should be limited in time and circumstances.[92] Both the OPC and the Commonwealth Ombudsman considered that exempt entities should be encouraged to adopt information-handling standards that are similar to those contained in the *Privacy Act*.[93]

30.52 The Australian Federal Police and the Insurance Council of Australia submitted that current exemptions are appropriate.[94]

ALRC's view

30.53 There are considerably more exemptions from the *Privacy Act* than from privacy legislation in other comparable jurisdictions. More importantly, some of the exemptions either do not appear to be justified or are too broad. For example, the justification for the exemption that applies to some of the agencies listed under the FOI Act is unclear.[95] Similarly, there does not appear to be any sound policy basis for leaving unprotected the personal information contained in employee records.[96]

30.54 Even where an exemption is justified, sometimes its scope is too wide. For instance, media organisations are exempt in relation to activities done 'in the course of journalism', provided that they are publicly committed to certain privacy standards. The term 'journalism' and other key terms, however, are not defined. In addition, 'media organisation' is defined to mean an organisation whose activities consist of collecting, preparing or disseminating news, current affairs, information or documentary (and related commentary, opinion and analysis) to the public. Arguably, the use of the word 'information' separately from 'news', 'current affairs' and 'documentary' leaves the exemption too wide. The lack of criteria for media privacy standards also means that public commitment to any privacy statement—even one that

---

89 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
90 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007.
91 Government of South Australia, *Submission PR 187,* 12 February 2007.
92 K Pospisek, *Submission PR 104,* 15 January 2007.
93 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.
94 Australian Federal Police, *Submission PR 186,* 9 February 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.
95 See Ch 33.
96 See Ch 36.

has little substance—may allow an individual or organisation to take advantage of the exemption.[97]

30.55 Consistent with international standards, the ALRC considers that exemptions should be limited to the extent possible and justified on sound policy grounds. The ALRC agrees with the OPC and the Commonwealth Ombudsman that, even when partial or full exemptions from the *Privacy Act* are justified, the exempt entities should be encouraged to adopt information-handling practices that are, to the extent possible, consistent with the privacy principles. In the remaining chapters in Part E, the ALRC makes a number of proposals for reform that are intended to give effect to this policy position.

Complexity of the exemption provisions

30.56 Some commentators have argued that the exemption provisions in the *Privacy Act* are overly complex.[98] Such complexity makes it difficult to determine the extent to which individuals and entities are exempt from the Act.

30.57 Certain agencies are, in effect, completely exempt from the operation of the *Privacy Act*, but this is not readily apparent from the structure of the provisions. For example, while intelligence agencies fall within the definition of an 'agency', acts done, or practices engaged in, by them are not included in the acts or practices to which the Act generally applies.[99] In addition, s 7(2) of the *Privacy Act* provides that provisions in the Act *except* in respect of the IPPs, the NPPs, an approved privacy code and some of the Privacy Commissioner's functions *do not* apply to these agencies. Arguably, this exemption could be simplified by stating that intelligence agencies are completely exempt from the operation of the Act.

30.58 The acts and practices of a number of agencies and organisations initially fall outside the acts or practices to which the Act applies, but the extent of the exemption is then modified either within the same section or through another section. Further, the scope of some exemptions must be ascertained by reference to other legislation.

30.59 For example, the agencies listed under Schedule 2 Part II Division 1 of the FOI Act fall within the definition of an 'agency'. Section 7(1)(a)(i)(C) of the Act, however, appears to exempt their acts and practices completely. Section 7(1)(c) then provides that these acts and practices fall within the acts or practices to which the Act applies *except* in relation to records for which the agencies are exempt from the operation of the FOI Act. Further, s 7(2) of the *Privacy Act* provides that the provisions of the

---

97 See Ch 38.

98 T Dixon, 'Preparing for the New Privacy Legislation' (Paper presented at Australia's New Privacy Legislation, Baker & McKenzie Cyberspace Law and Policy Centre CLE Conference, Sydney, 24–25 May 2001); R Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (1989) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html> at 30 July 2007.

99 *Privacy Act 1988* (Cth) ss 6(1), 7(1)(a)(i)(B).

Privacy Act, except in respect of the IPPs, the NPPs, an approved privacy code and some of the Privacy Commissioner's functions, apply to these agencies. Finally, s 7A provides that, notwithstanding s 7(1)(a)(i), 7(1)(c) and 7(2), acts and practices done in relation to documents in relation to these agencies' commercial activities, or the commercial activities of another entity, are treated as acts and practices of an organisation.

30.60 The ambiguity of some of the exemption provisions has also given rise to criticism.[100] For example, small businesses are defined as businesses with an annual turnover of $3 million or less. It has been argued, however, that it is difficult for individuals to know the turnover of a business and, therefore, whether the business is exempt.[101]

Submissions and consultations

30.61 A number of stakeholders commented on the complexity of the exemption provisions of the *Privacy Act*,[102] and the need for a clear statement of the exemptions and their scope.[103] The Legal Aid Commission of New South Wales submitted that that the complexity of the existing exemptions

> introduce[s] a degree of uncertainty for people seeking remedial action under the Act. This can make it more difficult for legal aid organizations to provide advice on privacy remedies. This is contrary to the purpose of the legislation to provide clearly understandable standards which both sides to a transaction can use to negotiate fair use of personal information.[104]

30.62 Stakeholders expressed particular concern about the complexity of the exemptions provided for in s 7 of the *Privacy Act*.[105] For example, the OPC suggested that s 7 be redrafted because 'it is a very complex and difficult section to understand and apply', which makes it difficult for many entities to understand which aspects of

---

100 See, eg, Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000*, 3 September 2000; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000.

101 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 4; Australian Privacy Charter Council, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry on the Privacy Amendment (Private Sector) Bill 2000*, 20 August 2000. The small business exemption is discussed further in Ch 35.

102 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; SBS, *Submission PR 112,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

103 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

104 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

105 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

their activities are covered by the Act.[106] In contrast, while the ABC acknowledged that the 'carving out and partial reapplication' under s 7 is relatively complex, it suggested that the section has the advantage of indicating the relationship between these exemptions and those applying under the FOI Act.[107]

30.63 ASIO supported the simplification of the exemption provisions that apply to ASIO and other intelligence agencies, provided that it does not alter the scope of the exemption.[108]

ALRC's view

30.64 The ALRC agrees that the exemption provisions are overly complex. In particular, the exemption and the circumstances in which it does not apply under s 7 of the Act are unnecessarily complicated. Simplifying the exemption provisions would assist individuals and entities in understanding their rights and obligations under the *Privacy Act*.

30.65 In Chapter 3, the ALRC proposes that the Australian Government redraft the *Privacy Act* to achieve greater consistency, simplicity and clarity. This would include the redrafting of the exemption provisions to enhance their accessibility. Specific proposals for reform are also contained in the following chapters of Part E.

Location of the exemption provisions

30.66 The exemptions from the *Privacy Act* are contained in a number of provisions throughout the Act, including ss 6C–7C, 12A, 12B, 13A–13D and 16E. It can be argued that setting out the exemptions together in one part of the Act would make the exemption provisions more accessible. For example, exemptions under the FOI Act are set out in a schedule to that Act. This has the advantage of clarity as well as reinforcing the message that exemptions are not the primary focus of the legislation.

30.67 One stakeholder submitted that exceptions to the principles are preferable to exemptions, because the variety of ways in which an entity can be exempt from the *Privacy Act* makes it difficult for individuals to determine if an entity has breached its privacy obligations.[109]

30.68 Some overseas jurisdictions—such as the United Kingdom, New Zealand and Hong Kong—set out most of their exemption provisions in a specific part of the

106 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
107 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.
108 Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007.
109 Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

legislation.[110] Other jurisdictions, like the United States and Canada, group exemption provisions together in one section or consecutive sections.[111]

Submissions and consultations

30.69 In IP 31, the ALRC asked where exemption provisions should be located.[112] Of the few stakeholders who commented on this issue, most supported simplifying the exemptions by setting them out in a schedule to the Act.[113]

30.70 The OPC suggested a two-pronged approach. Where exemptions exist for certain categories of entities, the exemptions should be grouped together in one part of the Act. Where exemptions exist for specific, named entities, they should be listed in a schedule to the *Privacy Act*. This listing should distinguish between entities with a full exemption and those with partial exemptions.[114]

30.71 Another suggestion is for exempt entities to be listed in subordinate legislation, rather than in the *Privacy Act* itself. The Real Estate Institute of Australia submitted that both exempt entities and those entities specifically made subject to the *Privacy Act* should be listed in subordinate legislation on the basis that 'regular legislative reviews and changing community concerns are likely to result in ongoing changes to the status of [these] entities'. It stated that this would 'aid the modification of the Act over time, in recognition of the need for the *Privacy Act* to stay abreast of technological, social and political developments'.[115]

30.72 One submission suggested that exemptions should, where possible, be located within the privacy principles to which they relate.

> This approach (i) will help avoid a plain reading of a principle creating misleading expectations of coverage, and (ii) help avoid organisations being able to claim that they 'comply' with a principle, when in fact an exemption located elsewhere means the exact opposite outcome.[116]

---

110 See, eg, *Data Protection Act 1998* (UK) Part IV—Exemptions; *Privacy Act 1993* (NZ) Part 6—Codes of practice and exemptions from information privacy principles; *Data Protection Act 1988* (Ireland) s 1(4)(c); *Personal Data (Privacy) Ordinance* (Hong Kong) Part VIII—Exemptions.

111 *Privacy Act 1974* 5 USC § 552a (US) (j), (k); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2).

112 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–1.

113 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Confidential, *Submission PR 143,* 24 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

114 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

115 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

116 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

30.73 Telstra and the ABC submitted that the exemptions should remain where they are. While acknowledging that locating the exemptions in one part of the Act would make them more accessible, the ABC observed that stakeholders are now familiar with the layout of the Act.[117] Telstra stated that the cost of complying with amendments to the *Privacy Act* would far outweigh any benefit that would result from a more consistent layout of the Act.[118]

ALRC's view

30.74 Submissions indicated support for grouping the exemption provisions together, either in one part of the *Privacy Act* or in a schedule to the Act. The ALRC agrees with the two-pronged approach suggested by the OPC. Where exemptions for certain categories of entities or types of acts and practices exist, they should be grouped together in a separate part of the Act. Where exemptions for specific, named entities exist, they should be set out in a schedule to the Act. The schedule should set out clearly the scope of any such exemption. This approach would enhance the accessibility and clarity of the exemption provisions. The alternative approach of locating partial or full exemptions within specific privacy principles has the potential to render the principles overly complex and unwieldy.

30.75 Privacy legislation in some overseas jurisdictions groups exemptions under a separate part of the legislation—for example, Part IV of the *Data Protection Act 1998* (UK) and Part VIII of the *Data Protection (Privacy) Ordinance* (Hong Kong). The categories of entities or types of acts and practices that should be grouped together in a part of the *Privacy Act* include: federal courts; the exemption relating to personal use; the media exemption; and exemptions applying to related bodies corporate, change in partnership, and an act or practice that is required by foreign law.

30.76 In the interest of clarity, specific, named entities that are exempt from the *Privacy Act*—such as ASIO, the Australian Crime Commission and the Integrity Commissioner—should be set out in a schedule to the Act. This is consistent with the approach in the FOI Act. In relation to specific agencies that are exempt from both the *Privacy Act* and the FOI Act, they should be specified in the schedule to the *Privacy Act* instead of by reference to their exempt status under the FOI Act. This would avoid the need to refer to other legislation when determining the exempt status of particular agencies under the *Privacy Act*.

Proposal 30–1 The *Privacy Act* should be amended to group together in a separate part of the Act exemptions for certain categories of entities or types of acts and practices.

117 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.
118 Telstra, *Submission PR 185,* 9 February 2007.

Proposal 30–2 The *Privacy Act* should be amended to set out in a schedule to the Act exemptions for specific, named entities. The schedule should distinguish between entities that are completely exempt and those that are partially exempt from the *Privacy Act*. For those entities that are partially exempt, the schedule should specify those acts and practices that are exempt.

Part E

Exemptions

31. Defence and Intelligence Agencies

Contents

Introduction 899
The exempt agencies 900
Intelligence agencies 900
Defence agencies 901
Inspector-General of Intelligence and Security 902
Rationale for the exemption of the AIC agencies 903
Privacy requirements 903
Accountability and oversight mechanisms 910
Other accountability mechanisms 914
International instruments 916
Issues concerning the exemption of the IGIS 916
Submissions and consultations 918
AIC agencies 918
Inspector-General of Intelligence and Security 921
Other defence and intelligence agencies 922
ALRC's view 922

Introduction

31.1 The Australian intelligence community (AIC) comprises six Australian Government intelligence agencies—the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Office of National Assessments (ONA), the Defence Intelligence Organisation (DIO), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO). Collectively, these agencies (AIC agencies) work together to meet Australia's intelligence needs.[1]

31.2 Three of the AIC agencies are responsible for collecting intelligence outside Australia: ASIS is responsible for human intelligence obtained through interaction with people; the DSD for signals intelligence obtained by intercepting electronic

1 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 4.

communications—such as telephones, faxes and emails; and the DIGO for imagery and geospatial intelligence obtained from imaging satellites and other sources.[2]

31.3 The ONA and the DIO are responsible for foreign intelligence assessment. Their functions are to analyse and assess intelligence as well as information from other sources—such as the media, the internet and diplomatic reporting—to form a picture of an issue or occurrence.[3] In this chapter, ASIS, the DIGO, the DSD, the DIO and the ONA—that is, all the AIC agencies except ASIO—are collectively referred to as 'the foreign intelligence agencies'.

31.4 ASIO, as a security intelligence agency, mainly focuses on the domestic security of Australia. Unlike the foreign intelligence agencies—which have either an intelligence collection or assessment role but not both—ASIO has both an intelligence collection and an assessment role.[4]

31.5 Currently, the AIC agencies are either partially or completely exempt from the *Privacy Act 1988* (Cth). This chapter examines whether they should continue to be exempt.

The exempt agencies

Intelligence agencies

31.6 Under the *Privacy Act*, intelligence agencies are defined to mean ASIO, ASIS and the ONA.[5] Acts and practices of these agencies are completely exempt from the operation of the *Privacy Act*.[6] A record that has originated with, or has been received from, an intelligence agency is also excluded from the operation of the Act.[7] Accordingly, agencies and organisations receiving a record from an intelligence agency are exempt from the operation of the *Privacy Act* in relation to that record. In addition, disclosure of personal information to ASIO or ASIS is not covered by the Act.[8]

31.7 ASIO's main role is to gather information and produce intelligence, enabling it to warn the government about risks to national security. It also provides security assessments, gives protective security advice and collects foreign intelligence in Australia.[9] The *Australian Security Organisation Act 1979* (Cth) (ASIO Act) defines 'security' as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on

---

2 Ibid, 3.
3 Ibid, 3.
4 Ibid, 3–4.
5 *Privacy Act 1988* (Cth) s 6(1).
6 Ibid s 7(1)(a)(i)(B), (2)(a).
7 Ibid s 7(1)(f).
8 Ibid s 7(1A)(a), (b).
9 Australian Security Intelligence Organisation, *About ASIO* <www.asio.gov.au/About/Content/what.aspx> at 31 July 2007; *Australian Security Intelligence Organisation Act 1979* (Cth) s 17.

Australia's defence system and acts of foreign interference.[10] ASIO falls within the portfolio responsibilities of the Attorney-General of Australia.

31.8 ASIS is Australia's overseas intelligence collection agency. Its role is to collect and distribute foreign intelligence that may impact on Australian interests, undertake counter-intelligence activities and liaise with overseas intelligence and security agencies.[11] ASIS is responsible to the Australian Government through the Minister for Foreign Affairs.[12] Under the *Intelligence Services Act 2001* (Cth), the Director-General of ASIS is directly responsible to the Minister.[13]

31.9 The ONA was established by the *Office of National Assessments Act 1977* (Cth) as an independent agency accountable to the Prime Minister. It produces assessments and reports on international political, strategic and economic matters in order to assist the Prime Minister, ministers and departments in the formation of policy and plans.[14] The Director-General of ONA is an independent statutory office holder, and as such is not subject to external direction on the content of assessments by the ONA.[15]

Defence agencies

31.10 The Defence Intelligence Group in the Department of Defence consists of three units: the DSD, the DIGO and the DIO. They are exempt from the operation of the *Privacy Act* where their acts and practices relate to their activities.[16] Records that have originated with, or have been received from, these agencies are also excluded from the operation of the Act.[17] Accordingly, agencies and organisations receiving a record from these agencies are exempt from the operation of the *Privacy Act* in relation to that record. Furthermore, disclosure of personal information to the DSD is not covered by the Act.[18]

31.11 The functions of the DSD and the DIGO, and certain limits on their activities, are set out in the *Intelligence Services Act*. The DSD is the national authority on security of information on communications and information systems across government. Its principle functions are to collect and communicate foreign signals

10 *Australian Security Intelligence Organisation Act 1979* (Cth) s 4.
11 Australian Secret Intelligence Service, *About ASIS's Role* <www.asis.gov.au/about.html> at 31 July 2007.
12 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 10.
13 *Intelligence Services Act 2001* (Cth) s 18.
14 Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007.
15 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 8.
16 *Privacy Act 1988* (Cth) s 7(1)(ca).
17 Ibid s 7(1)(g).
18 Ibid s 7(1A)(c).

intelligence, and provide advice to the Australian Government on the security of information kept in electronic form.[19]

31.12 The DIGO provides intelligence information derived from imagery and other sources in support of Australia's defence and national interests.[20] It is responsible for providing imagery and geospatial intelligence to help meet Australia's foreign intelligence requirements, supporting the operations of the Australian Defence Force, and supporting the national security function of Australian Government and state and territory authorities.[21]

31.13 The DIO provides intelligence assessments based on information from other Australian and foreign intelligence agencies to support the Department of Defence, the planning and conduct of defence force operations, and wider government decision making.[22] There is no legislation specific to the DIO, although some of its activities are covered under the *Intelligence Services Act*.[23]

Inspector-General of Intelligence and Security

31.14 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office within the Prime Minister's portfolio. The IGIS was set up under the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act) to ensure that certain intelligence and security agencies conduct their activities within the law, behave with propriety, comply with ministerial guidelines and directions, and have regard to human rights. He or she regularly monitors the activities of AIC agencies, conducts inquiries, investigates complaints about these agencies, makes recommendations to the government and provides annual reports to the Australian Parliament.[24]

31.15 The IGIS, as an agency listed in Schedule 2 Part I Division 1 of the *Freedom of Information Act 1982* (Cth), is exempt from compliance with the Information Privacy Principles (IPPs).[25] He or she is, however, subject to other provisions of the Act, such as the tax file number provisions. In addition, as an exempt agency under the *Freedom of Information Act*, the IGIS is not required under that Act to provide access to information.

---

19 Australian Government Department of Defence, *Defence Signals Directorate—About DSD* <www.dsd.gov.au/about_dsd/index.html> at 31 July 2007.

20 Australian Government Department of Defence, *Defence Imagery and Geospatial Organisation—About DIGO* <www.defence.gov.au/digo/about.htm> at 31 July 2007.

21 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 11.

22 Australian Government Department of Defence, *Defence Intelligence Organisation* <www.defence.gov.au/dio/index.html> at 31 July 2007.

23 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 5.

24 Inspector-General of Intelligence and Security, *Frequently Asked Questions* <www.igis.gov.au/faq's.cfm> at 31 July 2007.

25 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2).

Rationale for the exemption of the AIC agencies

31.16 The IGIS has stated that one of the reasons why the Australian intelligence agencies should be exempt or partially exempt from the provisions of the *Privacy Act* is that 'it is necessary for the agencies to protect their sources, capabilities and methods if they are to function effectively'.[26] Other reasons for the exemption include that: there are already adequate privacy requirements on the AIC agencies contained in legislation, ministerial directions and guidelines; there are robust accountability and oversight mechanisms over the agencies; and the exemption is consistent with international standards. These reasons are discussed below.

Privacy requirements

Legislation

31.17 AIC agencies may only collect intelligence on Australians under warrant or authorisation by a responsible minister. As discussed below, the *Intelligence Services Act* sets out the circumstances in which the responsible minister may authorise intelligence activity by the three foreign intelligence collection agencies—ASIS, the DSD or the DIGO—against an Australian person.

31.18 Section 8 of the *Intelligence Services Act* provides that the responsible minister must issue a direction requiring ASIS, the DSD or the DIGO to obtain an authorisation under s 9 from the minister before undertaking intelligence activity on an Australian person. Section 32B of the IGIS Act requires the minister to give a copy of any such direction to the IGIS as soon as practicable after it is given. The validity of a ministerial authorisation given under s 9 is limited to no more than six months, and may only be renewed if the relevant minister is satisfied that it is necessary for the authorisation to continue to have effect.[27] A copy of the authorisation must be kept by the agency and made available for inspection on request by the IGIS.[28]

31.19 The agency heads of ASIS, the DIGO and the DSD must give to the responsible minister a written report in respect of intelligence activities carried out by the agency in reliance on a ministerial authorisation. The report must be provided to the minister within three months from the day on which the authorisation ceased to have effect.[29]

31.20 The *Intelligence Services Act* also sets out limits on the functions of ASIS, the DSD and the DIGO, which are only to be performed in the interests of Australia's national security, foreign relations and national economic well-being, and 'to the extent

---

26 Inspector-General of Intelligence and Security, 'Trust and the Rule of Law' (Paper presented at Australian Institute of Professional Intelligence Officers, Intelligence 2005 Conference, 3 November 2005), 4.

27 *Intelligence Services Act 2001* (Cth) ss 9(4), 10.

28 Ibid s 9(5).

29 Ibid s 10A.

that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'.[30] These three agencies are prohibited from undertaking any activity that is unnecessary for the proper performance of their functions, or not authorised or required by or under another Act.[31]

31.21 Generally, ASIO may only collect information relevant to security under warrant.[32] In addition, only the Director-General of Security or an ASIO officer authorised by the Director-General, can communicate intelligence on behalf of ASIO. It is an offence for an ASIO employee or agent to convey information acquired in the course of his or her duties outside ASIO without the authority of the Director-General of Security. The Director-General of Security may authorise an ASIO officer to communicate information to authorities of any other country approved by the Director-General.[33] Section 20 of the ASIO Act places a special responsibility upon the Director-General of Security to take all reasonable steps to ensure that the work of ASIO is limited to what is necessary for the purposes of the discharge of ASIO's functions.

Privacy rules and guidelines

Attorney-General's guidelines issued under the Australian Security Intelligence Organisation Act 1979 (Cth)

31.22 Under s 8A of the ASIO Act, the Attorney-General may give the Director-General of Security guidelines to be observed by ASIO in the performance of its functions or the exercise of its powers. The Attorney-General has issued two sets of guidelines concerning ASIO's functions—one in relation to obtaining intelligence relevant to security,[34] and another in relation to politically motivated violence (referred to collectively as the 'Attorney-General's Guidelines').[35] Both sets of guidelines contain privacy standards for the treatment of personal information.

31.23 The Attorney-General's Guidelines require that the collection of information 'be conducted with as little intrusion into privacy as is possible, consistent with the national interest'.[36] They provide that the degree of intrusion into individual privacy

---

30 Ibid s 11.

31 Ibid s 12.

32 *Australian Security Intelligence Organisation Act 1979* (Cth) pt III divs 2 and 3. The only exception is where an authorised ASIO officer or employee requests information or documents from an operator of an aircraft or vessel relating to its cargo, crew, passenger, stores or voyages: *Australian Security Intelligence Organisation Act 1979* (Cth) s 23.

33 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18–19.

34 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of its Function of Obtaining Intelligence Relevant to Security* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007.

35 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007.

36 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of its Function of Obtaining*

should be proportional to the gravity of the threat to security.[37] In deciding whether to conduct an investigation relating to politically motivated violence and the investigatory methods to be employed, the Director-General of Security is required to consider all of the circumstances, including the privacy implications of any proposed investigation.[38]

31.24 In addition, the Attorney-General's guidelines in relation to obtaining intelligence relevant to security provide that:

- the initiation and continuation of an ASIO investigation requires authorisation by the Director-General of Security or an ASIO senior executive officer;[39]
- ASIO must periodically review their investigations;[40]
- where an investigation concludes that a subject's activities are not relevant to security, the records of that investigation must be destroyed pursuant to disposal schedules agreed to between ASIO and the Australian Archives;[41]
- requests by ASIO for access to personal information held by Australian Government agencies should be 'limited to that which is reasonably necessary for the purposes of approved investigations';[42] and
- records must be kept of all: ASIO's requests for access to personal information; personal information received in response to such requests; and personal information communicated to a person or agency by ASIO incidental to the

---

Intelligence Relevant to Security <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007 Guideline 2.12; Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007, Guideline 3.2.

37 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of its Function of Obtaining Intelligence Relevant to Security* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007 Guideline 2.13; Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007, Guideline 3.9.

38 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation of its Functions relating to Politically Motivated Violence* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007, Guideline 3.6(d).

39 Australian Security Intelligence Organisation, *Attorney-General's Guidelines in relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of its Function of Obtaining Intelligence Relevant to Security* <www.asio.gov.au/About/Content/AttorneyAccountability.aspx> at 31 July 2007, Guidelines 2.7–2.9.

40 Ibid, Guidelines 2.16–2.17.

41 Ibid, Guideline 2.18.

42 Ibid, Guideline 4.1.

obtaining of intelligence, including 'to whom the material was communicated, by whom and for what purpose'.[43] The records are to be open to inspection by the IGIS and, where appropriate, subject to an authorised disposal schedule under the *Archives Act 1983* (Cth).[44]

31.25 The IGIS has oversight responsibility to ensure that ASIO complies with the Attorney-General's Guidelines in conducting its activities. During 2005–06, the IGIS reported that his office inspected records associated with a wide range of ASIO activities, including warrant operations and authorisations of investigation. The IGIS has inspected every authorisation that was issued during the reporting period. His inspections showed that most requests for authorisation were 'completed to a high standard'. In relation to the requirement under the Attorney-General's Guidelines that ASIO periodically review authorities to investigate, the IGIS reported that compliance with this requirement was generally good. He noted several instances where reviews had not been completed within a reasonable timeframe and also some minor procedural defects, but did not consider that there were any systemic concerns.[45]

31.26 The ALRC has been advised that the Attorney-General's Guidelines are currently being updated.

Privacy rules issued under the Intelligence Services Act 2001 (Cth)

31.27 Under s 15 of the *Intelligence Services Act*, the responsible minister is required to make written rules regulating the communication and retention by the DIGO, the DSD and ASIS of intelligence information concerning Australians. Before making the rules, the responsible minister must consult with the head of the relevant agency as well as the IGIS and the Attorney-General.

31.28 The current privacy rules for ASIS, the DSD and the DIGO are broadly consistent with each other.[46] The rules provide for the circumstances in which the agency may communicate and retain intelligence information concerning an Australian person. In addition, they provide that where the agency has communicated intelligence information concerning an Australian person contrary to the rules or because it had wrongly presumed that a person was not an Australian person, the agency shall immediately consult with or inform the IGIS of the measures taken to protect the

43 Ibid, Guidelines 4.2, 4.4.

44 Ibid, Guideline 4.5.

45 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006), 30.

46 R Hill, *Defence Imagery and Geospatial Organisation Privacy Rules* (2005) Australian Government Department of Defence <www.defence.gov.au/digo/pdf/DIGOprivacyrules.pdf> at 31 July 2007; P Reith, *Defence Signals Directorate: Privacy Safeguards* (2001) Australian Government Defence Signals Directorate <www.dsd.gov.au/about_dsd/privacy_safeguards.html> at 31 July 2007; A Downer, *Australian Secret Intelligence Service: Rules to Protect the Privacy of Australians* (2001) Australian Secret Intelligence Service <www.asis.gov.au/rules_to_privacy.html> at 31 July 2007.

privacy of the Australian person.[47] The rules, however, do not require the agency to observe particular standards when engaging in other information-handling practices that are dealt with in the Information Privacy Principles (IPPs), such as accuracy, storage and security of personal information.

31.29 In his annual report for 2005–2006, the IGIS reported that his inspection work showed that compliance by ASIS and the DSD with the *Intelligence Services Act* and the associated privacy rules has been 'sound'.[48] He stated that his office undertook on-going monitoring of ASIS's compliance with privacy rules. He also regularly reviewed reports containing secret intelligence information to ensure that the information was collected in accordance with the requirements of the *Intelligence Service Act* and the privacy rules. The IGIS reported that 'the internal resources and training made available to ASIS staff on privacy issues are good, and that the obligations imposed by the privacy rules are taken very seriously'.[49] The IGIS stated that:

> I am pleased to say that I have seen no abuses in the material we have access to, rather there is a deepening understanding of the principles upon which the privacy rules are based and a continuing commitment by ASIS staff to do the right thing.[50]

31.30 In relation to the DSD, the IGIS reported that a fully staffed Office of Compliance section within the DSD monitors that the requirements of the privacy rules are being met, and his office fulfils a similar function independently of the DSD. He stated that there is a regular dialogue between the DSD and his office on privacy issues due to the inherently complex nature of the DSD's collection activities. The IGIS is, however, satisfied that

> the incidence of Australian persons being identified in DSD reporting is extremely low relative to the number of reports DSD disseminates. In some cases this occurs because DSD is not aware that the person holds Australian citizenship or permanent residency (commonly having dual nationality). As soon as DSD become aware of their status corrective action is taken.[51]

31.31 The IGIS further reported that the DSD has continued its sustained effort to train all staff in the requirements imposed by the *Intelligence Service Act*, and that his office has delivered 11 presentations to DSD staff on the role of his office and the principles underpinning the application of the privacy rules.[52]

---

47 R Hill, *Defence Imagery and Geospatial Organisation Privacy Rules* (2005) Australian Government Department of Defence <www.defence.gov.au/digo/pdf/DIGOprivacyrules.pdf> at 31 July 2007, r 6.

48 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006), viii.

49 Ibid, 38–39.

50 Ibid, 39.

51 Ibid, 45.

52 Ibid, 46.

31.32 During 2005–2006, the IGIS visited DIGO headquarters periodically and 'closely examined all tasking requests DIGO receives which might impact upon Australian persons or interests'. He reported that the adoption of new privacy rules by the DIGO on 2 December 2005 presented some unique challenges, due to the DIGO's predominantly image-based reporting. The IGIS stated, however, that his office would continue to work with the DIGO to address these issues. The IGIS was satisfied that all necessary approvals and authorisations were obtained under the relevant privacy rules.[53]

Administrative privacy guidelines

31.33 Unlike ASIS, the DSD and the DIGO, the ONA and the DIO are not required by legislation to have privacy rules or guidelines in place. A review of the *Intelligence Services Act* in 2005–06 coordinated by the Australian Government Department of the Prime Minister and Cabinet resulted in a government decision that the ONA and the DIO should be subject to privacy guidelines consistent with the requirements placed on ASIS, the DSD and the DIGO. The ONA and the DIO have since developed and implemented privacy guidelines that are broadly consistent with those in use elsewhere in the AIC. Both sets of guidelines have been in effect since December 2005.[54]

31.34 The purpose of the guidelines is to ensure that in the agencies' external communications, the privacy of Australians is preserved as far as is consistent with the proper performance of the agencies' functions.[55] The guidelines for the ONA and the DIO constitute a direction to all agency staff by the responsible Minister.[56] Copies of the guidelines are annexed to the IGIS's Annual Report for 2005–06, but are not currently available on the website of the ONA or the DIO.[57]

31.35 In his annual report for 2005–06, the IGIS reported that he was consulted by the ONA and the DIO in the development of the privacy guidelines. He has also worked with both agencies during the implementation of the guidelines to ensure that the guidelines were applied in a manner consistent with use elsewhere in the AIC. The IGIS reported that both the ONA and the DIO embarked on an organisation-wide program to educate analysts on applying the guidelines and reporting on compliance with the guidelines. The IGIS was satisfied with both the implementation of the guidelines and the level of awareness of the guidelines among analysts.[58]

31.36 During the reporting period 2005–06, the IGIS conducted one inspection of the use of the guidelines by the ONA and another by the DIO, and was 'pleased with the overall quality and level of detail contained in the documentation'. The IGIS stated that

---

53 Ibid, 49.
54 Ibid, 8.
55 Ibid, Annex 6 (DIO), Annex 7 (ONA).
56 Ibid, 8.
57 Ibid, Annex 6 (DIO), Annex 7 (ONA). The Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006) is available on the IGIS's website <www.igis.gov.au>.
58 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2005–2006* (2006), 50–51, 53–54.

he intended to conduct inspections relating to the use of the privacy guidelines by the DIO and the ONA every three months.[59]

31.37 The IGIS stated that he would continue to monitor compliance with the privacy rules and guidelines by the foreign intelligence agencies.[60]

Protective Security Manual

31.38 In addition to privacy rules and guidelines that apply to the individual agencies, all the AIC agencies are required to comply with the *Protective Security Manual*. The *Protective Security Manual* is a policy document produced and periodically revised by the Australian Government Attorney-General's Department on behalf of the Protective Security Policy Committee.

> It is the principal means for disseminating Australian Government protective security policies, principles, standards and procedures, to be followed by all Australian Government agencies for the protection of official resources.[61]

31.39 The *Protective Security Manual* sets out guidelines and minimum standards in relation to protective security for Australian Government agencies and officers, as well as for contractors and their employees who perform services for the Australian Government. Of particular relevance is Part C of the *Protective Security Manual*, which provides 'guidance on the classification system and the protective standards required to protect both electronic- and paper-based security classified information'.[62] This part sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

31.40 Although the *Protective Security Manual*—as it applies to the AIC agencies—addresses some of the privacy issues that are not dealt with under the AIC agencies' privacy rules or guidelines, the privacy protections under the *Protective Security Manual* guidelines are restricted to security classified information and do not deal with other matters under the IPPs, such as the accuracy of personal information.

31.41 The DSD also publishes an unclassified version of the *Australian Government Information Technology Security Manual* (ACSI 33).[63] This document provides guidance to Australian Government agencies on the protection of their electronic information systems.

---

59 Ibid, 50–51, 53–54.
60 Ibid, 56–57.
61 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 31 July 2007.
62 Ibid.
63 Defence Signals Directorate, *Australian Government Information Technology Security Manual (ACSI 33)* (2004).

31.42 In its report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recommended that a revised *Protective Security Manual* be placed in the public domain, with any sensitive security information removed.[64] In September 2005, the Attorney-General's Department released a revised *Protective Security Manual*. The availability of the manual, however, remains restricted to Australian Government agencies. The ALRC continues to be of the view that the *Protective Security Manual* should be a publicly available document, as recommended in ALRC 98.

Secrecy provisions

31.43 Sections 39, 39A and 40 of the *Intelligence Services Act* prohibit the communication of any information or matter that was prepared by or on behalf of ASIS, the DIGO or the DSD in connection with their functions.[65] These provisions apply to a person who: is a current or former staff member of ASIS, the DIGO or the DSD; has entered into a contract, agreement or arrangement with one of these agencies; or has been an employee or agent of a person who has entered into a contract, agreement or arrangement with one of these agencies.

31.44 Similarly, it is an offence for an ASIO employee or agent to convey information acquired in the course of his or her duties outside ASIO without the authority of the Director-General of Security.[66]

Accountability and oversight mechanisms

31.45 Whether AIC agencies should continue to be exempt from the operation of the *Privacy Act* depends, in part, on whether current accountability principles and oversight mechanisms adequately address privacy issues.

Inspector-General of Intelligence and Security

31.46 As discussed above, the IGIS is an independent statutory officer who is responsible for ensuring that the AIC agencies conduct their activities legally, behave with propriety, comply with any directions and guidelines from the responsible minister, and have regard for human rights, including privacy. To ensure the independence of the office, the IGIS is appointed by the Governor-General for a fixed term of five years and can only be dismissed on limited grounds.[67] An IGIS cannot be appointed more than twice.[68]

31.47 The IGIS conducts inquiries, investigates complaints, makes recommendations to government and provides annual reports to the Australian Parliament. Sections 8 and 11 of the IGIS Act allows the IGIS to undertake inquiries in response to a complaint, at

---

64 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–1.

65 *Intelligence Services Act 2001* (Cth) s 39.

66 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18.

67 *Inspector-General of Intelligence and Security Act 1986* (Cth) ss 6(2), 26, 30.

68 Ibid s 26(2).

the request of the responsible minister or on the IGIS's own initiative, into a number of matters relating to the operations of the AIC agencies, including their compliance with the law, ministerial directions and guidelines, propriety and human rights standards.[69] The IGIS is directly accountable to the Prime Minister.

31.48 When exercising its inquiry function, the IGIS has significant powers that are similar to those of a Royal Commission. The IGIS has powers to obtain information, require persons to answer questions and produce documents, take sworn evidence and enter the premises of any AIC agency.[70] Under s 20 of the IGIS Act, the IGIS may obtain documents with a national security classification for the purposes of an inquiry but must make arrangements with the head of the relevant agency for the protection of those documents while they remain in the IGIS's possession, and for their return.

31.49 The IGIS has conducted several inquiries into the activities of AIC agencies, including inquiries into the: intelligence activities in relation to the Tampa incident; terrorist attacks in Bali in October 2002; allegations that the DSD intercepted communications of the Hon Laurie Brereton MP; and concerns raised about the DIO by Lieutenant Colonel Lance Collins.[71]

Ministerial oversight

31.50 The heads of the AIC agencies are responsible to their respective ministers in accordance with normal governance arrangements. The IGIS also assists ministers in their oversight of the AIC agencies by conducting inquiries into the agencies at the request of the ministers.[72]

31.51 In addition, the AIC agencies are guided by the National Security Committee, which sets broad policy and priorities for the agencies. The Committee is supported by the Secretaries Committee on National Security (SCNS), a committee of senior officials chaired by the Secretary of the Australian Government Department of the

---

69 Ibid ss 8, 11.

70 Ibid ss 18–20.

71 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2001–2002* (2002), Annex 2; Australian Government Inspector-General of Intelligence and Security, *Annual Report 2002–2003* (2003), Annex 2, 3; Australian Government Inspector-General of Intelligence and Security, *Annual Report 2003–2004* (2004), Annex 3, 4. See also Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 15. On 6 December 2000, Lieutenant Colonel Lance Collins of the Australian Defence Force wrote to the Minister for Defence expressing concerns that: the DIO acted in mid-1998 to quash early warning, included in an assessment prepared by him, of problems developing in East Timor; the DIO's assessments concerning East Timor were pro-Indonesia; and the DIO cut access to an intelligence database without warning. The IGIS was asked by the Minister for Defence to investigate, report and make recommendations about Collins' allegations. The IGIS found that Collins' view was sincerely held but unfounded: Australian Government Inspector-General of Intelligence and Security, *Annual Report 2003–2004* (2004), Annex 3.

72 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006).

Prime Minister and Cabinet and attended by the secretaries of the National Security Committee's portfolio departments and the Directors-General of the ONA and ASIO. The SCNS advises the National Security Committee on national security policy, coordinates implementation of policies and programmes relevant to national security, and guides departments and agencies involved in intelligence and security.[73]

Parliamentary oversight

31.52 Under s 29 of the *Intelligence Services Act*, the oversight responsibilities of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) include:

- reviewing the administration and expenditure of AIC agencies;
- reviewing any matter in relation to the AIC agencies referred to the Committee by the responsible minister or a resolution of either House of the Parliament; and
- reporting the Committee's comments and recommendations to each House of the Parliament and to the responsible minister.[74]

31.53 The AIC agencies are also subject to scrutiny by Senate legislation committees on their finance and administration, particularly their budget allocations. In addition, the IGIS is accountable to the Senate Finance and Public Administration Committee.[75]

31.54 ASIO produces an unclassified annual report for tabling in Parliament. It also provides a classified annual report to the Attorney-General, the Prime Minister and the Leader of the Opposition on its activities.[76] In the annual reports of the Department of Defence and the IGIS, broad references are made to the activities of the DIGO, DSD and the DIO. The heads of ASIS and the ONA must provide the responsible minister with a report on their operations at least annually.[77] Although these annual reports are not made public, both ASIS and the ONA do produce unclassified budget documents.[78]

Royal Commissions and other inquiries

31.55 AIC agencies have been the subject of several Royal Commissions and a number of other inquiries. The Hon Justice Robert Hope conducted two Royal Commissions into the AIC during the 1970s and 1980s, which broadly established the AIC's current structure, functions and processes. In March 1995, the Hon Gordon Samuels QC and Michael Codd concluded a Royal Commission that inquired into the

---

73 Ibid, 14.

74 The Committee also has responsibilities for reviewing the operation, effectiveness and implications of: certain amendments to anti-terrorism legislation; and ASIO's questioning and detention powers under Division 3 of Part III of the ASIO Act: *Intelligence Services Act 2001* (Cth) s 29(1)(ba), (bb).

75 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 14.

76 *Australian Security Intelligence Organisation Act 1979* (Cth) s 94.

77 *Intelligence Services Act 2001* (Cth) s 42; *Office of National Assessments Act 1977* (Cth) s 19.

78 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 15.

effectiveness of ASIS's organisation, management, control and accountability arrangements, protection of sources and resolution of grievances and complaints.[79]

31.56 The Parliamentary Joint Committee on ASIO, ASIS and DSD (now the PJCIS) conducted a number of inquiries into intelligence issues, including: an inquiry into the intelligence on Iraqi's weapons of mass destruction;[80] reviews of intelligence services legislation;[81] an assessment of the government's proposed amendment of the ASIO Act;[82] and an examination of the nature, scope and appropriateness of ASIO's public reporting activities.[83]

31.57 In 2004, the Prime Minister appointed Philip Flood to conduct an inquiry into the effectiveness of the intelligence community's current oversight and accountability mechanisms, and the delivery of high quality and independent intelligence advice to the government. In the 2004 *Report of the Inquiry into Australian Intelligence Agencies* (Flood Report),[84] it was acknowledged that all elements of government, including the AIC, should be accountable. The Report stated, however, that different accountability and oversight mechanisms for intelligence agencies are justified because of the need for parts of the intelligence function to remain secret. The Flood Report stated that purpose-specific institutions and systems are needed to deal with the tension between accountability and secrecy.[85] The Report found that accountability arrangements for the intelligence agencies were working effectively and that the *Intelligence Services Act* has worked well in practice.[86]

31.58 The Flood Report did, however, recommend some changes to the accountability arrangements in the AIC, including that: the mandate of the Parliamentary Joint Committee on ASIO, ASIS and DSD (now the PJCIS) be extended to cover all AIC agencies; the functions and ministerial accountabilities of the DIGO be formalised in

---

79 Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service* (1995).

80 Parliament of Australia—Parliamentary Joint Committee on ASIO ASIS and DSD, *Intelligence on Iraq's Weapons of Mass Destruction* (2003).

81 Parliament of Australia—Joint Select Committee on the Intelligence Services, *An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and Certain Parts of the Cybercrime Bill 2001* (2001); Parliament of Australia—Parliamentary Joint Committee on ASIO ASIS and DSD, *Review of the Intelligence Services Amendment Bill 2003* (2004); Parliament of Australia—Parliamentary Joint Committee on ASIO, ASIS and DSD, *Review of the Intelligence Services Legislation Amendment Bill 2005* (2005).

82 Parliament of Australia—Parliamentary Joint Committee on the Australian Security Intelligence Organization, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999* (1999); Parliament of Australia—Parliamentary Joint Committee on ASIO ASIS and DSD, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002* (2002).

83 Parliament of Australia—Joint Select Committee on the Intelligence Services, *A Watching Brief: The Nature, Scope and Appropriateness of ASIO's Public Reporting Activities* (2000).

84 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet.

85 Ibid, 51.

86 Ibid, 57.

legislation by amendments to the *Intelligence Services Act*; and the mandate of the IGIS be extended to allow the IGIS to initiate inquiries into matters relating to the ONA and the DIO without ministerial referral.[87] All of these recommendations have been implemented.

31.59 In *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the ALRC and the Administrative Review Council (ARC) were also of the view that scrutiny by the IGIS and the Parliamentary Committee on ASIO of the internal processes and methods of intelligence agencies is adequate.[88] They therefore recommended that intelligence agencies remain exempt from the operation of the *Freedom of Information Act*.[89]

Other accountability mechanisms

Commonwealth Ombudsman

31.60 The Commonwealth Ombudsman is an independent statutory office established by the *Ombudsman Act 1976* (Cth). The Act provides that the Ombudsman is to investigate the administrative actions of Australian Government departments and prescribed authorities in response to complaints or on the Ombudsman's own motion. The Act also permits the Ombudsman, in some circumstances, to decline to investigate; for example, where a matter has not yet been put to the relevant agency. The *Ombudsman Act* enables the Ombudsman to report in a number of ways following an investigation, although it requires the investigation itself to be conducted in private and with fairness to anyone likely to be criticised.

31.61 The Australian Government Attorney-General's Department and the Departments of Defence, Foreign Affairs and Trade, and the Prime Minister and Cabinet are within the Ombudsman's jurisdiction. ASIO and the IGIS, however, are excluded. The foreign intelligence agencies fall within the Ombudsman's jurisdiction but, in practice, people seeking to make complaints about them are referred to the IGIS.[90] The Ombudsman is also appointed as the Defence Force Ombudsman under the *Ombudsman Act*.[91]

31.62 The Act provides the Ombudsman with an extensive range of powers to investigate, including a power to require the production of information or documents.[92] This power is limited, however, by s 9(3), which provides that the Attorney-General may issue a certificate certifying that the disclosure to the Ombudsman of certain information or documents would be contrary to the public interest for a number of

87 Ibid, 59–60.
88 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [11.13].
89 Ibid, Rec 74.
90 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [2.43].
91 *Ombudsman Act 1976* (Cth) s 19B.
92 Ibid s 4.

reasons—including that it would prejudice the security, defence or international relations of the Australian Government.

Security Appeals Division of the Administrative Appeals Tribunal

31.63 The Security Appeals Division of the Administrative Appeals Tribunal (AAT) deals with three types of matters, namely, applications for review of:

- adverse or qualified security assessments undertaken by ASIO;
- decisions of the Australian Archives under the *Archives Act 1983* (Cth) in respect of access to a record of ASIO; and
- preventative detentions orders issued or extended under the *Criminal Code*. [93]

31.64 The AAT, however, does not have power to review security assessments conducted by agencies other than ASIO.

31.65 Under the ASIO Act, a security assessment cannot be made in respect of a person who is not: an Australian citizen; the holder of a valid permanent visa; or the holder of a special category or special purpose visa.[94] During review by the AAT, ASIO is required to provide applicants with access to personal information held about the individual provided the disclosure of such information is not likely to prejudice security.[95]

Australian National Audit Office

31.66 The Australian National Audit Office (ANAO) is a specialist public sector agency responsible for auditing the activities of most Australian Government public sector entities. The Auditor-General has broad information-gathering powers and authority to access Australian Government premises.[96] The scope of its audit program includes all of the AIC agencies.[97] The ANAO undertakes annual audits of the financial statements of ASIO, ASIS and the ONA. It also conducts audits of the Department of Defence that broadly consider the financial operations of the DIO, the DSD and the DIGO. In addition, the ANAO undertakes occasional performance audits

---

93 *Administrative Appeals Tribunal Act 1975* (Cth) s 19(6); *Australian Security Intelligence Organisation Act 1979* (Cth) s 54; *Criminal Code Act 1995* (Cth) s 105.51(6). See also G Downes, 'The Security Appeals Division of the Administrative Appeals Tribunal—Functions, Powers And Procedures' (Paper presented at National Security Law Course, University of Sydney, Sydney, 13 September 2006).

94 *Australian Security Intelligence Organisation Act 1979* (Cth) s 36.

95 *Administrative Appeals Tribunal Act 1975* (Cth) ss 36, 37(1AE), 39A.

96 *Auditor-General Act 1997* (Cth) pt 5 div 1.

97 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 16.

of programmes relevant to the intelligence agencies, normally as part of broader cross-government work on security issues.[98]

Opposition briefing

31.67 Section 21 of the ASIO Act requires that the Director-General of Security brief the Leader of the Opposition for the purpose of keeping him or her informed on matters relating to security. Similarly, the Director-General of ASIS must consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to ASIS.[99]

International instruments

31.68 A number of international instruments recognise the need to balance the interests of national security and defence with the interests of privacy or data protection. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines) provides that acceptable bases for exceptions in the Guidelines include national sovereignty and national security.[100]

31.69 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains exemptions concerning public security, defence and state security.[101]

31.70 Similarly, the *Asia-Pacific Economic Cooperation Privacy Framework* (APEC Privacy Framework) states that it is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests. It does, however, provide that exceptions to the principles—including those relating to national sovereignty, national security, public safety and public policy—should be limited and proportional to meeting the objectives to which the exceptions relate, and made known to the public or in accordance with law.[102]

Issues concerning the exemption of the IGIS

31.71 As discussed above, agencies listed under Schedule 2 Part I of the *Freedom of Information Act*—of which the IGIS is one—are exempt from compliance with the IPPs. No policy justification has been given for the IGIS's exemption from the *Privacy*

---

98 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet, 57.

99 *Intelligence Services Act 2001* (Cth) s 19.

100 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4; Memorandum, [46].

101 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 3(2), 13; recitals 16, 43.

102 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

Act. Therefore, the exemption appears to derive from the fact that the IGIS is listed under Schedule 2 Part I of the *Freedom of Information Act*.

31.72 In their 1994 inquiry into the *Freedom of Information Act*, the ALRC and ARC commented that decisions to exempt particular agencies from the *Freedom of Information Act* have tended to be selective.[103] However, in view of the fact that if the IGIS and other intelligence agencies were subject to the Act the vast majority of its documents would be exempt, the ALRC and ARC recommended that the IGIS and other intelligence agencies should remain in Part I of the Act as exempt agencies.[104]

31.73 Currently, there are no privacy rules or guidelines that apply to the IGIS. The IGIS is, however, required to comply with the *Protective Security Manual* and is subject to secrecy provisions. Part C of the *Protective Security Manual* sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information. The privacy protections under the *Protective Security Manual*, however, are restricted to security classified information and do not deal with other matters under the IPPs, such as the accuracy of personal information. In relation to secrecy, under the IGIS Act, the IGIS or a staff member is prohibited from making a record, or divulging or communicating any information acquired by reason of the person holding or acting in that office.[105]

31.74 The IGIS is directly accountable to the Prime Minister and must provide the Prime Minister with a report on the IGIS's activities annually. The Prime Minister may make deletions from the IGIS's annual report before tabling it in Parliament, if he or she considers that the deletion is necessary 'to avoid prejudice to security, the defence of Australia, Australian's relations with other countries or the privacy of individuals'. A full copy of the report is provided to the Leader of the Opposition, who must treat as secret any part of the report that is not tabled in Parliament.[106]

31.75 In Canada and New Zealand, bodies overseeing the work of security and intelligence agencies are subject to privacy legislation, but may refuse to disclose personal information under certain circumstances. In Canada, the Office of the Inspector General of the Canadian Security Intelligence Service and the Security Intelligence Review Committee are subject to federal privacy legislation.[107] They may, however, refuse to disclose any personal information requested if the information was obtained or prepared by any government institution that is a specified investigative

---

103 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

104 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 74.

105 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34.

106 Ibid s 35.

107 *Privacy Act* RS 1985, c P-21 (Canada) s 3 (definition of 'government institution').

body in the course of lawful investigations relating to activities suspected of constituting threats to the security of Canada.[108]

31.76 Similarly, in New Zealand, the Inspector-General of Intelligence and Security and the Intelligence and Security Committee are covered by the *Privacy Act 1993* (NZ). They may, however, refuse to disclose any information if the disclosure would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand, or the entrusting of information to the Government of New Zealand on a basis of confidence by foreign governments, their agencies or any international organisation.[109]

31.77 In contrast, in the United Kingdom, personal data are exempt from any of the data protection principles and other provisions of the *Data Protection Act 1998* (UK) if the exemption from that provision is required for the purpose of safeguarding national security.[110]

Submissions and consultations

AIC agencies

31.78 In the Issues Paper *Review of Privacy* (IP 31), the ALRC asked whether the AIC agencies should be exempt, either completely or partially, from the *Privacy Act*; and if so, what is the policy justification for the exemption.[111] A number of submissions considered that the current exemption is appropriate,[112] provided that there is oversight by a body with sufficient power and authority over the practices of the AIC agencies.[113]

31.79 Submissions from the Office of the Privacy Commissioner (OPC) and the AIC agencies supported the view that some of the Information Privacy Principles (IPPs) are incompatible with the functions of the AIC agencies.[114] In a joint submission, the foreign intelligence agencies stated that:

---

108 Ibid s 22.

109 *Privacy Act 1993* (NZ) s 27.

110 *Data Protection Act 1998* (UK) s 28.

111 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–2.

112 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007; Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007.

113 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; W Caelli, *Submission PR 99,* 15 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007.

114 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007; Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007.

> The collection and communication of information or opinions about people and entities and their activities is a core element of the business of intelligence. At times, and in line with strict statutory provisions…, this may involve the collection and/or communication of information about Australian persons or entities. This information is collected for specific purposes relevant to the intelligence requirements of government.
>
> There may be security and other factors which constrain intelligence agencies from informing the individual concerned about the information collected ([IPP] 2) or obtaining their consent before disclosing that information to another agency ([IPP] 11, paragraph 1(b)). Disclosure can prejudice collection methods, reveal to individuals and organisations that they are of interest to the collection agencies and also enable intelligence targets to employ defensive security measures that would hinder the collection of intelligence. A strict compliance with the *Privacy Act* would, therefore, unduly constrain the ability of intelligence agencies to carry out their functions.[115]

31.80 ASIO submitted that requiring it to comply with the requirements of the *Privacy Act*—and, in particular, the principles in relation to collection (IPPs 2 and 3), access (IPP 6) and consent (IPP 10)—would be inconsistent with the requirement of security:

> They would significantly undermine ASIO's investigations by alerting persons of security interest of the fact of, and scope of, covert investigations. The requirements of the Privacy Act present a risk of disclosure of ASIO's methods, capabilities and sources to persons of security interest. Further, the requirements would undermine ASIO's domestic and international liaison relationships as partner agencies would be likely to withhold the sharing of intelligence where there is a requirement for ASIO to disclose this information to persons of security interest.[116]

31.81 The OPC and the AIC agencies also expressed the view that there are currently adequate privacy requirements on the AIC agencies, including legislative requirements, ministerial directions and secrecy provisions.[117] In addition, the foreign intelligence agencies submitted that:

> As a matter of practice, intelligence agencies have invested in resources to ensure that the rules are adhered to. Individual agencies also conduct internal audits to monitor the use of the relevant privacy guidelines and to ensure that appropriate care is being taken to protect information pertaining to Australian persons, in accordance with legislative and administrative requirements.[118]

31.82 Furthermore, submissions from ASIO and the foreign intelligence agencies stated that the AIC agencies are already subject to robust accountability and oversight

---

115 Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007.

116 Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007.

117 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007; Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007.

118 Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007.

mechanisms, including through the IGIS and the PJCIS.[119] By contrast, the Queensland Council of Civil Liberties expressed concern that there is a danger that intelligence agencies may regard themselves as exempt from control and supervision, and suggested that other mechanisms should be sought to ensure that these agencies are accountable.[120]

31.83 The OPC noted that there may be difficulties if the Privacy Commissioner were empowered to investigate or audit the activities of AIC agencies:

> it may be difficult for the Privacy Commissioner to investigate or audit the activities of AIC agencies without the appropriate powers, infrastructure or security clearances to conduct such investigations. It appears that the IGIS has been developed as a specialist monitoring and review body for these agencies given the different nature of their work.[121]

31.84 In addition, ASIO suggested that the current exemption that applies to it is consistent with international standards under the OECD Guidelines, the EU Directive and the APEC Privacy Framework.[122]

31.85 The Centre for Law and Genetics submitted that 'it is not unreasonable that these agencies be exempt', but the exemption should only apply when an officer of an AIC agency is acting in the public interest, and not when he or she is seeking out information for private purposes. It also suggested that, as a matter of good practice, any access to personal information by these agencies should be recorded to enable access to be tracked and later audited.[123]

31.86 On the other hand, a few stakeholders suggested that, although there is a legitimate public interest in exempting the AIC agencies from compliance with the *Privacy Act*, these agencies should not be completely exempt from the Act.[124] For example, the Australian Privacy Foundation stated that 'no agency, however important the public policy purpose it is performing, should be exempt from the obligation to comply with fundamental human rights and administrative law principles'. It submitted that:

> there is no justification for these agencies not to be subject to all of the principles in respect of administrative and employment information, or for them to be exempt

---

119 Ibid.
120 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.
121 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
122 Australian Security Intelligence Organisation, *Submission PR 180,* 9 February 2007.
123 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
124 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; K Pospisek, *Submission PR 104,* 15 January 2007.

> from, for example, the security and quality principles, even for the personal information they collect operationally.[125]

31.87 Similarly, the Commonwealth Ombudsman submitted that the public interest justification for the exemption might not necessarily extend to staff or contractor records.[126]

31.88 The Australian Privacy Foundation, Professor Graeme Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that:

> The fact that access, correction and review and complaint rights might need to be qualified for operational data does not justify lifting the obligation to keep information secure, maintain data quality and delete information once no longer required. The reasonable steps qualification to these principles should adequately deal with the special circumstances of these agencies.
>
> Similarly there is no reason why the use and disclosure principles should not apply, with a specific exception similar to that provided in the context of access in NPP 6.1(k) in addition to the normal range of required by law and 'prejudice to law enforcement' exceptions.[127]

Inspector-General of Intelligence and Security

31.89 In IP 31, the ALRC asked whether the agencies specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act*—including the IGIS—should be exempt from the *Privacy Act*; and if so, what is the policy justification for the exemption.[128]

31.90 To date, no stakeholders have specifically commented on the exemption that applies to the IGIS in submissions and consultations. Several stakeholders suggested, however, that the exemption of any Australian Government agencies, including those specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act*, should be justified and limited to the extent possible.[129] Greenleaf, Waters and Bygrave submitted that any difficulties that compliance with privacy principles might cause for such agencies should be dealt with by means of selective exceptions to particular principles.[130]

---

125 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

126 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.

127 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

128 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.

129 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

130 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

Other defence and intelligence agencies

31.91 In IP 31, the ALRC also asked whether any other defence and intelligence agencies should be exempt from the *Privacy Act*.[131] Except the foreign intelligence agencies, no other stakeholders have commented on this issue. The foreign intelligence agencies noted that the Defence Security Authority, which is a member of the Intelligence and Security Group, is not exempt from the *Privacy Act*. They did not see any reason, however, for the Defence Security Authority to be exempt from the Act.[132]

ALRC's view

31.92 Only a small number of submissions commented on the exemption that applies to the AIC agencies. Those who have commented acknowledged the need to balance the interests of individual privacy with the interests of national security and defence. This is consistent with international standards, which provide for exceptions or exemptions to privacy principles for the purposes of national security and defence.

31.93 The central function of AIC agencies is the covert collection and assessment of intelligence information—that is, information 'obtained without the authority of the government or group that "owns" the information'.[133] Given the inherently covert nature of much of the work of these agencies, many of the requirements under the privacy principles would be incompatible with their functions—especially those relating to the collection, use and disclosure of personal information, and specific notification to the individual concerned about the information collected.

31.94 Although the AIC agencies are partially or completely exempt from the *Privacy Act*, each of these agencies has privacy rules or guidelines in place. Compliance with these rules and guidelines are overseen by the IGIS, who has reported his overall satisfaction with their implementation and compliance by the AIC agencies.

31.95 While compliance with the privacy rules and guidelines by the AIC agencies appears to be adequate, the ALRC considers that there is room for extending the ambit of the privacy rules and guidelines, and improving the relevant legislative arrangements and the accessibility of the rules and guidelines.

31.96 First, the governing legislation, and privacy rules and guidelines that apply to the AIC agencies only cover collection, communication and retention of intelligence information. The *Protective Security Manual* does contain minimum standards

---

131 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–2.

132 Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 31 July 2007. The Defence Security Authority is responsible for the development of security policy, security training and awareness across the Department of Defence and the Australian Defence Force, security performance assessment programs, serious and complex security investigations, and processing of the majority of the Defence's security clearances.

133 Office of National Assessments, *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight* (2006), 3.

concerning the use, access, copying, storage, security and disposal of classified information. It only applies to security classified information, however, and does not deal with other matters under the IPPs. Therefore, the ALRC is of the view that the privacy rules and guidelines should be updated to include rules dealing with the incorrect use and disclosure of personal information, the accuracy of records, and the storage and security of personal information.

31.97 Secondly, under the ASIO Act and the *Intelligence Services Act*, the responsible ministers for ASIO, ASIS, the DSD and the DIGO are required to make written rules regulating the communication and retention of intelligence information concerning Australian persons. Although the ONA and the DIO have implemented administratively privacy guidelines, they are not subject to the same requirement legislatively as other AIC agencies. The ALRC considers this anomaly should be corrected by an amendment to the *Intelligence Services Act* and the *Office of National Assessments Act*.

31.98 Furthermore, although some of responsible ministers for the AIC agencies are required to consult with the IGIS and the Attorney-General in making privacy rules, none of them are required to consult with the OPC in making such rules. The ALRC's view is that it would be desirable for all ministers with responsibility for the AIC agencies to consult with the OPC before making privacy rules.

31.99 Finally, although all privacy rules and guidelines applicable to the AIC agencies are currently available electronically on the IGIS's website, and some of them are available on the relevant agency's website, those applicable to the ONA and the DIO are not currently available on their website. The ALRC is of the view that all privacy rules and guidelines should be published on the relevant agency's website.

31.100 A few stakeholders have suggested that the AIC agencies should be subject to exceptions to specific privacy principles, rather than exemption from the *Privacy Act*. However, all the AIC agencies are already subject to privacy rules or guidelines. The ALRC is also proposing extending the ambit of these rules and guidelines to further enhance privacy protection. In addition, the internal processes and methods of the AIC agencies are subject to a number of oversight and accountability mechanisms, including the IGIS, the PJCIS and other bodies. In particular, the IGIS has reported that he conducted regular inspections of the AIC agencies and actively monitored their adherence to privacy rules and guidelines. In this regard, it should be noted that the OPC would have difficulties investigating or auditing the activities of the AIC agencies, given the nature of their work. For these reasons, the ALRC does not consider it necessary to alter the scope of the exemption that applies to the AIC agencies under the *Privacy Act*.

31.101 In relation to the IGIS, much of the personal information being handled would have originated with, or have been received from, an AIC agency. Although these

records are excluded from the operation of the *Privacy Act*, other records held by the IGIS may also contain security sensitive information—for example, such information may be contained in the IGIS's internal working documents that relate to the work of the AIC agencies. Accordingly, the ALRC is of the view that some exemption from the *Privacy Act* should continue to apply to the IGIS.

31.102 There is, however, no policy justification for the exemption to extend to the IGIS's administrative records. Unlike the AIC agencies, the IGIS is not bound by ministerial privacy rules or guidelines and its operations are not subject to oversight other than by the Prime Minister. The ALRC proposes, therefore, that the IGIS be brought under the *Privacy Act* in respect of his or her office's administrative operations, such as the handling of employee records. In addition, the IGIS, in consultation with the Privacy Commissioner, should develop and publish information-handling guidelines. This would ensure that the privacy of personal information handled by the IGIS in respect of his or her office's non-administrative operations is also protected adequately.

Proposal 31–1 The privacy rules and guidelines, which relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, Australian Security Intelligence Service, Defence Imagery and Geospatial Organisation, Defence Intelligence Organisation, Defence Signals Directorate and Office of National Assessments, should be amended to include consistent rules and guidelines relating to:

(a) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of the incident and measures taken to protect the privacy of the Australian person);

(b) the accuracy of personal information; and

(c) the storage and security of personal information.

Proposal 31–2 Section 15 of the *Intelligence Services Act 2001* (Cth) should be amended to provide that:

(a) the responsible minister in relation to the Defence Intelligence Organisation is required to make written rules regulating the communication and retention by the Defence Intelligence Organisation of intelligence information concerning Australian persons; and

(b) before making rules to protect the privacy of Australian persons, the ministers responsible for the Australian Security Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Defence Intelligence Organisation should consult with the Office of the Privacy Commissioner.

Proposal 31–3 The *Office of National Assessments Act 1977* (Cth) should be amended to provide that:

(a) the responsible minister in relation to the Office of National Assessments (ONA) is required to make written rules regulating the communication and retention by the ONA of intelligence information concerning Australian persons; and

(b) before making rules to protect the privacy of Australian persons, the minister responsible for the ONA should consult with the Office of the Privacy Commissioner.

Proposal 31–4 Section 8A of the *Australian Security and Intelligence Organisation Act 1979* (Cth) should be amended to provide that, before making rules to protect the privacy of Australian persons, the responsible minister should consult with the Office of the Privacy Commissioner.

Proposal 31–5 The privacy rules and guidelines referred to in Proposal 31–1 should be made available electronically to the public; for example, on the websites of those agencies.

Proposal 31–6 The *Privacy Act* should be amended to apply to the Inspector-General of Intelligence and Security (IGIS) in respect of the administrative operations of that office.

Proposal 31–7 The Inspector-General of Intelligence and Security, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by IGIS is protected adequately.

32. Federal Courts and Tribunals

Contents

Introduction 927
Federal courts 927
Scope of the current exemption 927
Non-party access to court records 933
Party and witness access to court records 941
Federal tribunals 942
Industrial tribunals 942
Other federal tribunals 943
Application of the IPPs to federal tribunals 946
Other jurisdictions 946
Submissions and consultations 947
ALRC's view 951

Introduction

32.1 Federal courts are currently exempt from the operation of the *Privacy Act 1988* (Cth) in respect of matters of an administrative nature. The Australian Industrial Relations Commission (AIRC), and the Industrial Registrar and Deputy Industrial Registrars are also similarly exempt. Other federal tribunals, on the other hand, are not exempt. This chapter examines whether these agencies should be exempt from the operation of the Act.

Federal courts

Scope of the current exemption

32.2 Federal courts—including the High Court of Australia, the Federal Court of Australia, the Federal Magistrates Court of Australia and the Family Court of Australia[1]—fall within the definition of 'agency' in the *Privacy Act*.[2] They are covered by the Act, however, in respect of those of their acts and practices that relate to matters

1 The Industrial Relations Court of Australia is also a federal court. As a consequence of the *Workplace Relations and Other Legislation Amendment Act 1996* (Cth), however, the court's jurisdiction has been transferred to other courts. Despite the transfer of jurisdiction, the Industrial Relations Court continues to exist at law until the last of its judges resigns or retires from office: Federal Court of Australia, *Industrial Relations Court of Australia* <www.fedcourt.gov.au> at 1 August 2007.

2 *Privacy Act 1988* (Cth) s 6(1).

'of an administrative nature'. Therefore, acts and practices of the federal courts in relation to their administrative records—including personnel records, operations and financial records, freedom of information records, complaint files and mailing lists—are covered by the *Privacy Act*.[3] Acts and practices in relation to the courts' judicial records, including court lists, judgments and other documents kept by the courts in relation to proceedings, are exempt.[4]

32.3 The partial exemption of federal courts from the operation of the *Privacy Act* was said to be based on two principles: the doctrine of the separation of powers, which is embodied in the structure of the *Australian Constitution*; and the common law principle of open justice. The separation of powers requires that different institutions exercise the legislative, judicial and executive powers of the Commonwealth, and that no one institution should exercise the power or functions of the others.[5] The principle of open justice requires that, subject to limited exceptions to protect the administration of justice, court proceedings should be open to the public.[6] Public access to court proceedings is vital to maintaining public confidence in the administration of justice.[7] Privacy issues arise, however, because personal information may be produced in court as a result of coercive powers and may be information that would not otherwise have entered the public arena.[8]

32.4 Certain information about matters before a court will generally be in the public arena and therefore often available to non-parties, such as court lists and judgments. Court lists may include file numbers enabling linkage to other information held in the justice system. Court lists can be highly prejudicial to individuals because they record court appearances rather than outcomes.[9] Court judgments containing sensitive personal information may be recorded in law reports and computerised legal databases and become available to the public.[10] Other case information, such as correspondence

---

3 Ibid s 7(1)(b); *I v Commonwealth Agency* [2005] PrivCmrA 6.

4 *Privacy Act 1988* (Cth) s 7(1)(a)(ii); *I v Commonwealth Agency* [2005] PrivCmrA 6. In *Re Bienstein and Family Court of Australia* [2006] AATA 385, the Administrative Appeals Tribunal (AAT) held that the organisation of court lists and the allocation of judicial officers to particular cases are not matters of an administrative nature, but 'matters affecting litigants and the public, and are intimately related to the independent and impartial administration of justice': *Re Bienstein and Family Court of Australia* [2006] AATA 385, [8].

5 *New South Wales v Commonwealth* (1915) 20 CLR 54; *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254; *Attorney-General (Cth) v The Queen* (1957) 95 CLR 529.

6 *Scott v Scott* [1913] AC 417; *Dickason v Dickason* (1913) 17 CLR 50; *Russell v Russell* (1976) 9 ALR 103.

7 *Attorney-General (UK) v Leveller Magazine Ltd* [1979] AC 440, 450. See also 'A Mutual Contempt? How the Law is Reported' (2005) 32(11) *Brief* 12, 16.

8 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 54.

9 Ibid, 55.

10 In *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83, the AAT considered how much personal information the Tribunal may publish in its decisions. Deputy President Forgie decided that, pursuant to IPP 11, the Tribunal was required or authorised by law to disclose as much personal information as is necessary to meet the requirements of s 43(2B) of the *Administrative Appeals Tribunal Act 1975* (Cth), including the obligation to conduct its proceedings and decision making in public, or to disclose the intellectual processes it followed in reaching a decision.

between the courts and the parties, is generally not in the public arena but is kept on file in court registries.

Matters of an administrative nature

32.5 The *Privacy Act* does not define 'a matter of an administrative nature'. The definition of 'administration' in the *Macquarie Dictionary* suggests that 'administrative' means relating to 'the management or direction of any office or employment'.[11] In administrative law, it has been held that the expression 'decision of an administrative character' is 'incapable of precise definition' and is to be 'determined progressively in each case as particular questions arise'.[12]

32.6 Given that a comprehensive definition of 'administrative' is not possible, the courts have taken the approach of defining 'administrative' by distinguishing it from legislative and judicial actions.[13] The distinction between administrative, legislative and judicial actions, however, is also difficult. In *Evans v Friemann*, Fox ACJ stated that 'it has … proved very difficult, virtually impossible to arrive at criteria which will distinguish in all cases' the administrative, the legislative and the judicial.[14] In addition, it was said that the concepts at times overlap or merge into one another.[15] Nevertheless, a general categorisation is that:

> Legislative acts usually involve the formulation of new rules of law having general application. Judicial acts generally entail determinations of questions of law and fact in relation to disputes susceptible of determination by reference to established rules or principles … Ministerial acts usually involve the performance of a public duty, but in circumstances where little or no discretion is legally permissible.[16]

32.7 One approach to distinguishing between judicial and administrative functions is to differentiate between what is 'truly ancillary to an adjudication by the court', which is incidental to the exercise of judicial power; and other functions that are not truly ancillary, which are administrative.[17]

> In the judicial sphere, there are many incidental functions, essentially of an administrative nature, and even of a legislative nature which are regarded as being within the judicial power of the Commonwealth, because they are incidental to, or incidents of, the exercise of judicial power.[18]

---

11 *Macquarie Dictionary* (online ed, 2005).
12 *Hamblin v Duffy* (1981) 34 ALR 333, 338–339.
13 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005), [2.4.25].
14 *Evans v Friemann* (1981) 35 ALR 428, 433.
15 *Hamblin v Duffy* (1981) 34 ALR 333, 338; *Evans v Friemann* (1981) 35 ALR 428, 433.
16 *Hamblin v Duffy* (1981) 34 ALR 333, 338.
17 C Enright, *Federal Administrative Law* (2001), [22.129]; *Kotsis v Kotsis* (1970) 122 CLR 69, 92.
18 *Evans v Friemann* (1981) 35 ALR 428, 433.

32.8 A function that is 'truly ancillary to an adjudication by the court'

> must be truly subservient to adjudication. They must be undertaken pursuant to a direction by the court for the purpose of either quantifying and giving effect to an adjudication already made by the court, or of providing material upon the basis of which an adjudication by the court is to be made.[19]

32.9 In the context of freedom of information applications, case law suggests that documents that relate to matters of a non-administrative nature include: 'documents of the court which relate to the determination of particular matters, such as draft judgments, pleadings, documents returned under summons',[20] unrevised and unpublished transcripts of proceedings,[21] and notes relating to the provision of conciliation counselling by an officer of the court.[22]

Submissions and consultations

32.10 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether federal courts should remain exempt from the operation of the *Privacy Act*.[23] Some stakeholders considered the partial exemption that applies to federal courts appropriate.[24] It was submitted that the exemption reflects an appropriate balance between openness and the privacy needs of individuals.[25] The Centre for Law and Genetics stated that, while the lack of national consistency is problematic, it should be left to other legislation to impose restrictions on access to court documents and hearings.[26]

32.11 One stakeholder submitted that responsibility for matters relating to the exercise of the courts' jurisdiction 'is most appropriately vested in individual courts rather than through a national privacy regime'. It was submitted that this is 'a more nuanced, effective mechanism for protecting individuals' privacy than through the operation of national privacy laws that attach only to the nebulous concept of "administrative acts"'. In addition, it was submitted that:

> exposing [federal] courts to administrative review in respect of matters related to the progression, listing, management and hearing of, and records of decisions in cases under the control of judicial officers of the Court is inconsistent with the separation of the judicial and executive arms of government.[27]

---

19 *Kotsis v Kotsis* (1970) 122 CLR 69, 92.
20 *Re Altman and the Family Court of Australia* (1992) 27 ALD 369, 373.
21 Ibid; *Loughnan (Principal Registrar, Family Court of Australia) v Altman* (1992) 111 ALR 445.
22 *Re O'Sullivan and the Family Court of Australia* (1997) 47 ALD 765.
23 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
24 Confidential, *Submission PR 214,* 27 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
25 Confidential, *Submission PR 214,* 27 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
26 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
27 Confidential, *Submission PR 214,* 27 February 2007.

32.12 It was also noted that:

> Federal courts can, and do, utilise their rule-making powers to promulgate rules to protect individuals' privacy that are appropriate for their particular court (for example, rules governing access to court files).[28]

32.13 Some stakeholders submitted that the *Privacy Act* is not necessarily the appropriate instrument for resolving privacy concerns in relation to court records or proceedings.[29] The OPC noted that, while there are some privacy concerns about the publication of court records, especially in electronic format, the *Privacy Act* is not the appropriate instrument for 'implementing changes to protect the personal information contained in court records'. Instead, the OPC suggested that 'changes to court record publication are best dealt with through procedural directives or guidelines rather than through legislative intervention'.[30]

32.14 The Legal Aid Commission of New South Wales submitted that the *Privacy Act* 'is not necessarily the appropriate vehicle for resolving concerns about the way trials are conducted'. It stated, however, that:

> there is a privacy interest in limiting the availability of personal information in court records and judgments. Legal Aid NSW is aware of instances where spent convictions found in judgment databases have been used to harass the individuals concerned.[31]

32.15 Similarly, the Mental Health Legal Centre expressed concern about instances where personal information was disclosed in courts, including where: psychiatric reports have been read in open court by a magistrate; and details of a woman's identity and mental health information were released to the press in the Victorian Coroners Court.[32]

32.16 One stakeholder supported a total exemption of federal courts from the operation of the *Privacy Act*

> on the basis that the Courts themselves, either individually or collectively, would maintain a regime for protecting individuals' privacy as well as access to their records in appropriate cases through rules of court. This would provide federal courts with the flexibility to amend the rules to maintain the balance with the increasing take up by courts of technology, such as online filing, access through the internet to individual court records etc. Were it considered necessary to establish a common statutory framework for the regulation of information privacy in federal courts, appropriate provisions could be inserted directly into the relevant Acts of Parliament.[33]

---

28 Ibid.
29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
30 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
31 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
32 Mental Health Legal Centre Inc, *Submission PR 184,* 1 February 2007.
33 Confidential, *Submission PR 214,* 27 February 2007.

32.17 Some stakeholders submitted that the distinction between administrative and non-administrative matters lacks both clarity and precision.[34] One stakeholder stated that the distinction is 'extremely difficult to apply in practice', as some functions of the courts are neither clearly judicial nor administrative in nature, which is compounded by the fact that some functions overlap or merge into another.

> To achieve a sensible and more workable test it needs to be made to relate explicitly to the control of proceedings and steps in relation to proceedings … under the control of judicial officers.[35]

Options for reform

32.18 Given the difficulty in distinguishing between the judicial and administrative functions of courts, there are some options for reform that could be considered.

32.19 One option is to couch the exemption in positive terms, that is, exempting federal courts from the operation of the *Privacy Act* in respect of their judicial functions. This is the approach taken in New Zealand, New South Wales and the Northern Territory.[36] This approach, however, may limit the scope of the exemption where the function is not strictly judicial but is 'truly ancillary to an adjudication by the court'.[37]

32.20 Another option is to exempt federal courts in respect of their judicial and quasi-judicial functions. This is the approach used in Victoria and Tasmania.[38] The term 'quasi-judicial function', however, is also imprecise and may not be significantly different from a function that is 'truly ancillary to an adjudication by the court'.

32.21 A third option is either to define the word 'administrative' or the word 'judicial'. For example, the *Privacy and Personal Information Protection Act 1998* (NSW) relevantly provides that the 'judicial functions of a court' means:

> the functions of the court … as relate to the hearing or determination of proceedings before it, and includes:
>
> (a) in relation to a Magistrate—such of the functions of the Magistrate as relate to the conduct of committal proceedings, and
>
> (b) in relation to a coroner—such of the functions of the coroner as relate to the conduct of inquests and inquiries under the *Coroners Act 1980*.

ALRC's view

32.22 In the ALRC's view, federal courts should continue to be exempt in respect of matters of a non-administrative nature. The principal function of federal courts is to

---

34 Ibid; Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007.
35 Confidential, *Submission PR 214,* 27 February 2007.
36 *Privacy Act 1993* (NZ) s 32(1) (definition of 'agency'); *Privacy and Personal Information Protection Act 1998* (NSW) s 6; *Information Act 2002* (NT) ss 4 (definition of 'tribunal'), 5(5)(a).
37 *Kotsis v Kotsis* (1970) 122 CLR 69, 92.
38 *Information Privacy Act 2000* (Vic) s 10; *Personal Information Protection Act 2004* (Tas) s 7(a), (b).

hear and determine disputes, exercising the judicial power of the Commonwealth under Chapter III of the *Australian Constitution*. The partial exemption of federal courts from the *Privacy Act* is based on the separation of powers that is embodied in the *Australian Constitution*. It was intended to avoid interference with the independence of the judiciary and to foster the proper administration of justice. Exposing federal courts to administrative review of their judicial functions is inconsistent with the separation of judicial and executive arms of government.

32.23 In addition, there needs to be an appropriate balance between the interests of privacy and the principle of open justice. To achieve this balance, the ALRC considers that, in the exercise of their judicial functions, it is appropriate for federal courts to deal with the handling of personal information in their own procedural rules.

32.24 In respect of their administrative functions, courts should continue to be bound by the *Privacy Act*. While the ALRC acknowledges the inherent difficulty in distinguishing between judicial and administrative matters, it is not a reason for exempting federals court entirely from the operation of the Act. Given that the partial exemption of the courts is based in part on the separation of powers, there is no justification for exempting the courts in respect of their administrative operations.

32.25 The current approach in the *Privacy Act*—exempting federal courts 'except in respect of a matter of an administrative nature'—has one particular advantage, in that it mirrors the approach taken under the *Freedom of Information Act 1982* (Cth) (FOI Act). The FOI Act provides that it 'does not apply to any request for access to a document of the court unless the document relates to matters of an administrative nature'.[39] Although the term 'administrative' is imprecise, it has been judicially considered in relation to the FOI Act and, therefore, the current approach to the exemption is preferable to other approaches discussed above.[40]

Non-party access to court records

Public access to court records

32.26 Court records may contain sensitive personal information such as criminal history, psychiatric and psychological reports, and other medical records. Information on court records in relation to certain types of proceedings may also be particularly sensitive, for example, in family law, bankruptcy and criminal proceedings. In addition, children are considered to be particularly vulnerable and therefore the identification of children in court records raises specific privacy concerns.[41]

---

39 *Freedom of Information Act 1982* (Cth) s 5.

40 See, eg, *Re Altman and the Family Court of Australia* (1992) 27 ALD 369; *Loughnan (Principal Registrar, Family Court of Australia) v Altman* (1992) 111 ALR 445; *Re O'Sullivan and the Family Court of Australia* (1997) 47 ALD 765.

41 The identification of children in court records is discussed in Ch 60.

32.27 Although exempt from the *Privacy Act*, access to documents on file in court registries is regulated by other statutes or rules of court.[42] In the High Court, any person may inspect and take a copy of any document filed in the registry except: affidavits and exhibits to affidavits that have not been received in evidence in court; and documents that contain identifying information about a person where the disclosure of the identity of that person is prohibited by an Act, an order of the court or otherwise.[43]

32.28 In the Federal Court, a person can search and inspect documents specified in the *Federal Court Rules 1979* (Cth)—such as applications, pleadings, judgments, orders and submissions—unless the court or a judge has ordered that the document is confidential.[44] A person who is not a party to the proceeding may only inspect certain other documents with the leave of the court.[45] Leave will usually be granted, however, where a document has been admitted into evidence or read out in open court.[46]

32.29 In the Federal Magistrates Court, only specified persons may search or inspect the court's records without leave granted by the court or the registrar. Records relating to a family law or child support proceeding may only be searched or inspected by the Attorney-General, and other records related to a particular proceeding may only be searched or inspected by the parties, their lawyers or a child representative in the proceedings. Leave to search or inspect a record may only be granted to a person if he or she can demonstrate a 'proper interest'.[47]

32.30 In the Family Court, only specified persons may search, inspect or copy the court's records relating to a case without the permission of the court. The specified persons include: the Attorney-General, the parties and their lawyers, and independent children's lawyers. Permission to search, inspect or copy a court record may be granted to a person with a 'proper interest' in the case or the information in that particular court record.[48]

32.31 Access to court records may be affected by the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth). The Act enables information to be introduced during federal criminal and civil proceedings in an edited and summarised form to facilitate the hearing of a case without prejudicing national security and the right of the defendant to a fair trial. A court exercising federal jurisdiction must hold closed hearings in certain circumstances,[49] and must not make a record of the hearing

---

42 *High Court Rules 2004* (Cth) r 4.07.4.

43 See, eg, Ibid r 4.07.4; *Federal Court Rules 1979* (Cth) o 46 r 6; *Federal Magistrates Court Rules 2001* (Cth) r 2.08.

44 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).

45 Ibid o 46 r 6(3)–(5).

46 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au/courtdocuments/publicdocuments.html> at 30 July 2007.

47 *Federal Magistrates Court Rules 2001* (Cth) r 2.08.

48 *Family Law Rules 2004* (Cth) r 24.13.

49 *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ss 25, 27, 28, 38G, 38H.

available to, or allow the record to be accessed by, anyone except specified persons or entities.[50] The specified persons and entities include: the court hearing the appeal or reviewing the lower court's decision; the prosecutor in a criminal proceeding; the defendant's legal representative; an unrepresented party or a party's legal representative—provided that he or she has been given a security clearance at an appropriate level; and if the Attorney-General intervenes, the Attorney-General and his or her legal representatives.[51]

Media access to court records

32.32 Media reports are how most members of the public are made aware of court proceedings. Such reports necessarily depend on journalists having access to proceedings, either directly by being permitted to be present at the proceedings or indirectly by being allowed access to court records.

32.33 In *Raybos Australia Pty Ltd v Jones*, Kirby P stated that:

> The principles which support and justify the open doors of our courts likewise require that what passes in court should be capable of being reported. The entitlement to report to the public at large what is seen and heard in open court is a corollary of the access to the court of those members of the public who choose to attend … the principles which support open courts apply with special force to the open reporting of criminal trials and, by analogy contempt proceedings … [52]

32.34 Some legislation, however, recognises that certain proceedings may contain particularly sensitive information and should be subject to restricted media reporting. For example, s 121 of the *Family Law Act 1975* (Cth) makes it an offence, except in limited circumstances, to publish proceedings that identify persons or witnesses involved in family law proceedings. Section 91X of the *Migration Act 1958* (Cth) provides that the High Court, the Federal Court and the Federal Magistrates Court must not publish a person's name where the person has applied for a protection visa or a protection-related visa, or had such a visa cancelled.

Research access to court records

32.35 Research access may be considered an aspect of open justice because 'research offers a more considered and sustained evaluation of the way courts operate'.[53] Currently, none of the federal court rules specifically addresses the issue of researchers' access to court records. Researchers who seek access to court records that are not publicly accessible will be required to seek leave of the court, and in some

---

50 Ibid ss 29, 38I.
51 Ibid ss 29, 38I.
52 *Raybos Australia Pty Ltd v Jones* (1985) 2 NSWLR 47, 55, 58.
53 C Puplick, 'Justice: Now Open to Whom?' (2002) 6 *Judicial Review* 95, 105.

cases show that they have a proper interest in searching court records and inspecting court documents.[54]

32.36 The Family Court has a detailed policy in relation to the granting of research access to court records. The policy contains a number of requirements, including: the preservation of confidentiality of information; obtaining informed consent from study participants; restriction of access to medical or other treatment records, or other client data collection systems, to qualified clinical investigators; and clearance from an appropriate and credible ethics committee for certain types of studies. Applications for research access are considered by the Family Court's Research Committee, which makes recommendations to the Chief Justice and the Chief Executive Officer of the Family Court on whether access to the court's resources should be granted.

32.37 In its discussion paper on access to court records, the County Court of Victoria proposed a detailed process for approval of academic or commercial research utilising court records.[55] In its report on access to court records, the New Zealand Law Commission recommended that there be a single entry point for all requests for access to court records by researchers, and that the process and criteria for considering all research proposals be articulated fully and published.[56]

Harmonisation of court rules

32.38 In recent years, there has been some progress in the harmonisation of court rules in different areas of Australian law. The Council of Chief Justices and the Australian Institute of Judicial Administration have formed a Harmonisation of Rules of Court Committee. The Committee has harmonised rules of court in the area of corporations procedure, subpoenas, discovery of documents, and service of process outside the jurisdiction.[57] In 2001, the Federal Court and the Federal Magistrates Court completed a joint project to develop harmonised rules for bankruptcy proceedings.[58]

32.39 There are two ways in which court rules can be harmonised:

- vertical harmonisation, that is, harmonisation of the rules and procedures of courts within the same hierarchy, and
- horizontal harmonisation, that is, harmonisation of the rules and procedures of courts in different hierarchies, but which deal with the same subject matter, for example, federal, State and Territory courts when dealing with corporations matters.[59]

---

54 See, eg, *Federal Magistrates Court Rules 2001* (Cth) r 2.08(2).

55 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005), [28]. The Court stated that it would consider feedback on the discussion paper from court users and the general public in preparing its draft policy on access to court records: County Court of Victoria, *2005–06 Annual Report* (2006), 8.

56 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [8.40], rec R27.

57 Australian Government Attorney-General's Department, *Federal Civil Justice System Strategy Paper* (2003), 67.

58 Federal Magistrates Court of Australia, *Annual Report 2005–2006* (2006), 13, 18.

59 Australian Government Attorney-General's Department, *Federal Civil Justice System Strategy Paper* (2003), 66.

32.40 The purpose of harmonising court rules is 'to simplify legal procedures by removing unnecessary differences between courts'. The benefits of harmonisation are said to be: promoting a more efficient and less costly process for parties by removing the need for parties and practitioners to familiarise themselves with various procedural rules in different jurisdictions; and enhancing access to the courts by reducing complexity, inconvenience and expense.[60]

32.41 On the other hand, 'it can be argued that inappropriate harmonisation can discourage development of the law by stifling innovation and social experimentation'. Particular concerns have been expressed about the potential of vertical harmonisation to increase the cost of litigation in lower courts by introducing more complex rules. It has been said that some differences in court procedures could be of benefit to court users, particularly where lower courts may have simpler procedures specifically designed for less complex proceedings.[61]

32.42 In its 2003 strategy paper on the federal civil justice system, the Attorney-General's Department recommended 'that the courts continue to develop, where appropriate, uniform procedures for those areas of law in which the same jurisdiction can be exercised in more than one court'.[62]

32.43 The ALRC reviewed the issue of non-party access to court records as part of its inquiry into the protection of classified and security sensitive information. In its report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC identified a number of inconsistencies across state and federal court legislation and rules concerning public access to evidence and other court documents, including: the types of document that may be accessed; when public access can be presumed; whether leave of the court is required for access; and the release of transcripts to non-parties.[63] The ALRC recommended that the Standing Committee of Attorneys-General (SCAG) order a review of federal, state and territory legislation and court and tribunal rules relating to non-party access to evidence and other documents produced in relation to proceedings, with a view to developing and promulgating a clear and consistent national policy.[64]

Options for reform

32.44 There are a number of ways in which non-party access to court records could be standardised. One option is to grant different levels of access for different types of information on court records. In its discussion paper, *Review of the Policy on Access to*

---

60 Ibid, 66–67.
61 Ibid, 67.
62 Ibid, rec 4.
63 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [7.25], [7.36].
64 Ibid, Rec 7–1. This recommendation has not yet been implemented.

Court Information,[65] the Attorney General's Department of New South Wales proposed a system whereby court information is classified as either open to public access or restricted public access.[66] Restricted access information, such as social security and tax file numbers and driver's licence and motor vehicle registration numbers, would be subject to legislative prohibition against media publication.[67] Restricted access information would also be subject to the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW).[68]

32.45 A variation of this first approach is the recommendation in the report on access to court records prepared by the New Zealand Law Commission.[69] The New Zealand Law Commission recommended the enactment of a Court Information Act based on a presumption of open court records limited only by principled reasons for denying access,[70] including the protection of sensitive, private or personal information.[71]

32.46 Another option is to determine the level of access to court records by reference to the nature of the proceedings. In its discussion paper, *Access to Court Records*, the County Court of Victoria proposed that: non-party access to civil files generally be available unless the court orders otherwise; limited access to parties to criminal or appeal files, before and after the trial, at the discretion of the registrar on a case by case basis; and no access to criminal or appeal files by non-parties without an order of the court.[72]

32.47 A third option to regulate access to court records is to remove certain identifying information from the records before publication. In its report on privacy and public access to electronic case files, the Committee on Court Administration and Case Management (a committee of the Judicial Conference of the United States) recommended that civil and bankruptcy case files be made available electronically to the same extent they are available at the courthouse, provided that certain 'personal data identifiers' are modified or partially redacted.[73] In September 2003, the Judicial Conference further permitted remote public access to electronic criminal case files

---

65 New South Wales Government Attorney General's Department, *Review of the Policy on Access to Court Information* (2006).

66 Ibid, proposal 3.

67 Ibid, proposal 7.

68 Ibid, proposal 10. A prescribed agency may be authorised to obtain specified categories of restricted document provided that the agency is bound by protocols addressing the retention, use and security of the document.

69 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006).

70 Ibid, rec R6.

71 Ibid, rec R11.

72 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005), [14], [16], [18], [20].

73 Social security cases are to be excluded, however, from electronic access: Judicial Conference of the United States—Committee on Court Administration and Case Management, *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files* <www.privacy.uscourts.gov/Policy.htm> at 14 August 2007.

(with certain exceptions) if specified personal identifiers were edited.[74] Electronic access to court records is discussed further in Chapter 4.

Submissions and consultations

32.48 Some stakeholders were of the view that one set of principles for access to court records would be problematic.[75] One stakeholder submitted that 'any attempt to standardise arrangements for access to court records for the purposes of consistency, runs the risk of failing to take into account the nature and function of specialist courts and tribunals'. It was submitted that the principles related to accessing the files of specialist courts are influenced by public policy considerations different to those involved in accessing the files of courts that have broad jurisdiction, and that uniformity should not be achieved at the expense of the interests of persons involved or affected by litigation.[76]

32.49 The Legal Aid Commission of New South Wales submitted that:

> the right balance between access and disclosure of court records and judgements is not something that can be resolved by following a set of principles of general application. This is a further area where the Privacy Commissioner should be encouraged to prepare codes of practice or guidelines.[77]

32.50 In contrast, the OPC submitted that a coordinated approach between federal and state and territory courts would provide a more consistent framework for the electronic publication of court records. It suggested that, since the *Privacy Act* does not cover state and territory courts, the matter should be referred to SCAG, as recommended in ALRC 98.[78]

32.51 The Family Law Council suggested that police officers should have access to the Family Court's database so that officers could deal with cases of family violence that arise in the family law context—for example, where police are sent to recover a child from a parent who has wrongfully retained the child without much information about the circumstances surrounding the recovery orders issued by local magistrates. Another example is

---

74 Judicial Conference of the United States, *Judicial Privacy Policy Page* <www.privacy.uscourts.gov> at 14 August 2007. The Judicial Conference of the United States approved specific guidance for the implementation of the amended criminal policy in March 2004: Committee on Court Administration and Case Management—Criminal Law and Defender Services, *Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files* US Courts <www.privacy.uscourts.gov/crimimpl.htm> at 14 August 2006.

75 Confidential, *Submission PR 214,* 27 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

76 Confidential, *Submission PR 214,* 27 February 2007.

77 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

78 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

> where the court has ordered that a supervisor be present when a parent spends time with a child. Without access to information on the child related orders, police might attend a scene and remove the person responsible for supervising a parent spending time with a child without also removing the child as happened last year in Queensland. At the moment, police must rely on seeing the physical orders when they attend the scene.[79]

32.52 In relation to research access to court records, it was suggested in one submission that, although there is 'justifiable community interest' in the work of federal courts, access to court files by researchers should be regulated by the individual courts.[80]

ALRC's view

32.53 Since federal courts have differing jurisdictions, different considerations apply in relation to the levels of access to their records. For example, the Federal Court and the Federal Magistrates Court have broad jurisdiction, covering a wide range of matters. In contrast, the sensitive nature of the jurisdiction of the Family Court requires specific restrictions on access. It would be inappropriate to have one set of access rules for all federal courts. There is, however, merit in having the same access rules for courts in different hierarchies that deal with similar types of cases.

32.54 Currently, state and territory courts are excluded from the definition of 'organisation' and are not covered by the *Privacy Act*.[81] In the ALRC's view, a coordinated approach by federal, state and territory courts and tribunals would provide more consistency in respect of non-party access to court and tribunal records. The ALRC reaffirms its recommendation made in ALRC 98, that SCAG order a review of court and tribunal rules in relation to non-party access to court records, with a view to promoting a national and consistent policy.[82]

32.55 In relation to access by police officers to the Family Court's database in particular types of matters, the ALRC understands that the police are already allowed to do so under the *Family Law Rules 2004* (Cth). As mentioned above, under rule 24.13 of the *Family Law Rules*, with the permission of the court, a person is allowed to search, inspect or copy a document forming part of the court record if he or she can demonstrate a 'proper interest' in the case or the information in the court record. Police officers should not have any difficulty in demonstrating a proper interest in the course of carrying out of their law enforcement functions.

32.56 As for research access to court records, the ALRC considers that the principle of open justice is designed to promote research, given that research contributes to the understanding and improvement of the court system. Therefore, provided there are

---

79 Family Law Council, *Submission PR 269,* 28 March 2007.
80 Confidential, *Submission PR 214,* 27 February 2007.
81 *Privacy Act 1988* (Cth) s 6C(1), (3)(g).
82 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 7–1.

sufficient safeguards in place to ensure the proper handling of personal information, research should be encouraged. The Family Court already has such a policy, but it is not available on the court's website. Other federal courts have not published a written policy in relation to access to court records for research purposes. The ALRC proposes that federal courts that do not have such a policy should develop and publish one. Such policies should address issues concerning the privacy of court users, such as confidentiality, the need for informed consent by participants, restricted access to sensitive information, and approval by ethics committees where appropriate.

Proposal 32–1 Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.

Party and witness access to court records

32.57 Case files are accessible by parties and their legal representatives. One commentator has asked whether this right should extend to witnesses, on the basis that they are identified in the record and have the right to know what information is held about them.[83]

32.58 Another issue is whether parties should have the right to correct or annotate inaccurate or irrelevant material on the record. It has been argued that, since both freedom of information and privacy legislation gives individuals the right to correct information held about them in public records, the same rule should apply to court records.[84]

Submissions and consultations

32.59 One stakeholder submitted that witnesses should not be able to access court files because 'there is a real risk that the evidence and testimony of that witness may be affected by perusing the court file before giving his or her evidence', and where access to court records are restricted,

> the information held on the court file, even if inaccurate, is not publicly available and is therefore unlikely to be able to be accessed by or used by someone in a position to adversely affect the witnesses' interests. [85]

32.60 It was also submitted that allowing parties to correct or annotate inaccurate or irrelevant information on the court record 'may contaminate the court record, which is

83 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 55.
84 Ibid, 55.
85 Confidential, *Submission PR 214,* 27 February 2007.

meant to accurately reflect the material before the court rather than commentaries upon the evidence', and would represent a significant 'interference with the role and powers of Courts on appeal where additional evidence may be permitted, but only in limited circumstances'.

> Permitting annotations elevates the purpose of the court record from documents gathered to serve only the dispute resolution process to become an independent source of information which has intrinsic value in its own right. Treating court records in this way may lead to parties preparing documentation and presenting information in a form not only designed to facilitate the resolution of a dispute, but also with one eye to the court record itself forming a lasting repository of information. If this were the case issues the subject of judicial management or decision could be fought and refought by those dissatisfied with the outcome of proceedings and manifestly unable to move on in their lives. It is hard to see how this would be desirable.[86]

ALRC's view

32.61 The ALRC does not consider that parties and witnesses to proceedings should have the right to change or annotate court records. The purpose of court records is to reflect accurately the materials before the court for the purposes of the court's adjudicative functions. The nature of proceedings and the material collected in an adversarial system are inherently contentious. Allowing parties or witnesses to change or annotate court records would be a significant interference with the court's role as the arbiter of disputes. In addition, court records ought to reflect accurately the materials and evidence on which a court's decision is based, especially for the purposes of review on appeal.

32.62 Allowing witnesses to access court files during proceedings runs the risk that the evidence and testimony of witnesses may be affected before they give evidence. Witnesses are often ordered, at the discretion of the judge, to stay out of court in order to avoid the possibility that the testimony of a witness changes according to what has been seen and heard in court.[87] Similar considerations should apply in relation to court records.

Federal tribunals

Industrial tribunals

32.63 Agencies listed in Schedule 1 of the FOI Act are exempt from the *Privacy Act* except in relation to administrative matters.[88] These agencies include the AIRC, and the Industrial Registrar and Deputy Industrial Registrars. Another agency listed in

86 Ibid.

87 *R v Bassett* [1952] VLR 535; *R v Tait* [1963] VR 520, 523; *Moore v Registrar of Lambeth County Court* [1969] 1 All ER 782, 783; *R v Lister* [1981] 1 NSWLR 110, 114.

88 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(A), (b).

Schedule 1 of the FOI Act is the Australian Fair Pay Commission (AFPC). The AFPC is not a tribunal.[89] The exemption that applies to the AFPC is considered in Chapter 33.

32.64 The AIRC is an independent, national industrial tribunal established under the *Workplace Relations Act 1996* (Cth). The functions of the AIRC include: assisting employers and employees in resolving industrial disputes; handling certain termination of employment claims; rationalising and simplifying awards; and dealing with applications about industrial action.[90] The Industrial Registrar and Deputy Registrars provide administrative support to the AIRC. They also have responsibilities relating to the registration of unions and employer associations and their financial accountability.[91]

32.65 In performing its functions, the AIRC has certain powers, including the power to: inform itself in any manner it thinks appropriate; take evidence on oath or affirmation; conduct proceedings in private; summons any person to be present before the AIRC; compel the production of documents and other things; direct a person to attend a conference; and make interim and final decisions.[92]

Other federal tribunals

32.66 Other than the AIRC, no federal tribunals are exempt from the operation of the *Privacy Act*. Some examples of federal tribunals include: the Administrative Appeals Tribunal (AAT); the Migration Review Tribunal (MRT); the Refugee Review Tribunal (RRT); and the Social Security Appeals Tribunal (SSAT).

32.67 The AAT provides independent review of a wide range of administrative decisions made by the Australian Government and some non-government bodies. The AAT has jurisdiction to review decisions made under more than 400 separate Acts and legislative instruments, including decisions in the areas of social security, taxation, veterans' affairs and workers' compensation, bankruptcy, civil aviation, corporations law, customs, freedom of information, immigration and citizenship, industry assistance and security assessments undertaken by the Australian Security Intelligence Organisation.[93]

---

89 The AFPC is an independent, statutory body that is responsible for setting and adjusting federal minimum wages to promote the economic prosperity of the people of Australia: *Workplace Relations Act 1996* (Cth) s 23.

90 Ibid s 62; Australian Industrial Relations Commission, *About the Commission* <www.airc.gov.au> at 5 August 2007.

91 Australian Industrial Relations Commission, *About the Commission* <www.airc.gov.au> at 5 August 2007.

92 *Workplace Relations Act 1996* (Cth) ss 111, 115.

93 Administrative Appeals Tribunal, *About the AAT* <www.aat.gov.au/AboutTheAAT.htm> at 12 August 2007.

32.68 The AAT is generally required to hold hearings in public except where the AAT is satisfied that, by reason of the confidential nature of any evidence or matter or for any other reason, it is desirable for the hearing to be held in private.[94] The AAT may give directions prohibiting or restricting the: publication of the names and addresses of witnesses; publication of matters contained in documents lodged with, or received in evidence by, the AAT; and the disclosure to some or all of the parties of evidence given before the AAT, or of the content of a document lodged with, or received in evidence by, the AAT.[95] In addition, application for a review of a security assessment made to the Security Appeals Division of the AAT must be held in private.[96] The AAT also may restrict the publication of evidence and findings in the hearing of such an application.[97] The AAT is required to give reasons either orally or in writing for its decision, except in limited circumstances.[98]

32.69 Members and staff of the AAT are subject to a number of provisions prohibiting the disclosure of information in particular circumstances. These confidentiality obligations are found in the *Administrative Appeals Tribunal Act 1975* (Cth) and in other Acts and legislative instruments that confer jurisdiction on the AAT.[99]

32.70 The MRT is a merits review body established under the *Migration Act 1958* (Cth). The MRT provides a final, independent, merits review of visa and visa-related decisions made by the Minister for Immigration and Citizenship or, more typically, by officers of the Department of Immigration and Citizenship, acting as delegates of the Minister.[100] The MRT must conduct hearings in public, unless the tribunal considers that it is in the public interest to take evidence in private.[101] Examples of matters where an MRT review may be conducted in private include cases that involve allegations of children at risk of domestic violence, or sensitive information about the health of an individual.[102]

32.71 The RRT was also established under the *Migration Act*. It is an independent merits review tribunal, responsible for reviewing decisions made by the Department of Immigration and Citizenship to refuse or cancel protection visas to non-citizens in Australia. The RRT also has the power, in respect of certain 'transitory persons', to conduct an assessment of whether a person falls within the legal meaning of 'refugee'.[103] Unlike a court, the RRT is not adversarial. The Department is not usually

---

94 *Administrative Appeals Tribunal Act 1975* (Cth) s 35.
95 Ibid s 35(2).
96 Ibid s 39A(1).
97 Ibid s 35AA.
98 Ibid s 28.
99 See, eg, Ibid ss 66, 66A.
100 Australian Government Migration Review Tribunal, *About the Tribunal* <www.mrt.gov.au/about.htm> at 5 August 2007.
101 *Migration Act 1958* (Cth) s 365.
102 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007.
103 *Migration Act 1958* (Cth) s 411. See also Australian Government Refugee Review Tribunal, *About the Tribunal* <www.rrt.gov.au/about.htm> at 5 August 2007. A 'transitory person' is a person who has been in Australia for 6 months or more: *Migration Act 1958* (Cth) s 5.

represented at RRT hearings. The RRT is inquisitorial in nature and can obtain whatever information it considers necessary to conduct the review. All reviews before the RRT must be conducted in private.[104]

32.72 Both the MRT and RRT are subject to the same confidentiality requirements under the *Migration Act*. Sections 377 and 439 of the Act prohibit members and officers of the tribunals and interpreters from recording, communicating or divulging any information or documents about a person obtained in the course of exercising a function or duty under the Act, unless it is necessary for the performance of that function or duty or for the purposes of the Act. In addition, both tribunals have the power to restrict publication of information if it is in the public interest to do so.[105]

32.73 The SSAT is a statutory body established under the *Social Security (Administration) Act 1999* (Cth). It falls within the portfolio of the Minister for Families, Community Services and Indigenous Affairs. The role of the SSAT is to conduct merits review of administrative decisions made under social security law, family assistance law, child support law and various other pieces of legislation. It is the first level of external review of decisions made by Centrelink about social security, family assistance, education or training payments. It is also the first level of external review of most decisions made by the Child Support Agency.[106]

32.74 The SSAT must hear reviews in private, and directions may be given as to the persons who may be present at any hearing of a review. In giving such directions, the wishes of the parties and the need to protect their privacy must be considered.[107] The Executive Director of the SSAT may make an order directing a person who is present at the hearing not to disclose information obtained in the course of the hearing.[108] When the SSAT makes its decision on a review, it must prepare a written statement setting out the decision, the reasons for the decision and the findings on any material questions of fact, and refer to evidence and other materials on which the findings of fact were based.[109] A copy of the statement must be given to the parties to the review.[110] Members of the tribunals and interpreters are prohibited from recording, communicating or divulging any information or documents about a person obtained in the course of exercising a function or duty under the Act, unless it is necessary for the performance of that function or duty or for the purposes of the Act.[111]

---

104 *Migration Act 1958* (Cth) s 429.
105 Ibid ss 378, 440.
106 Australian Government Social Security Appeals Tribunal, *About the SSAT* <www.ssat.gov.au> at 5 August 2007.
107 *Social Security (Administration) Act 1999* (Cth) s 168.
108 Ibid s 169.
109 Ibid s 177.
110 Ibid s 177.
111 Ibid s 19.

Application of the IPPs to federal tribunals

32.75 Federal tribunals are currently able to rely on the exceptions to Information Privacy Principles (IPPs) 10 and 11 to use and disclose personal information in the course of exercising their functions.[112] IPPs 10 and 11 relevantly provide that an agency may use or disclose personal information where the:

- individual is aware, or reasonably likely to be aware, that information of that type is usually passed to a person, body or agency: IPP 11.1(a);
- individual has consented to the use or disclosure: IPPs 10.1(a), 11.1(b);
- record-keeper believes on reasonable grounds that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or other persons: IPPs 10.1(b), 11.1(c);
- use or disclosure is required or authorised by or under law: IPPs 10.1(c), 11.1(d);
- use or disclosure is reasonably necessary for enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue: IPPs 10.1(a), 11.1(e); or
- use of the information is directly related to the purpose for which it was obtained: IPP 10.1(e).

32.76 In addition, these tribunals' constituent Acts authorise the use and disclosure of personal information in certain situations.

Other jurisdictions

32.77 Some state privacy legislation provides that tribunals are exempt in relation to their judicial, quasi-judicial or decision-making functions. In New South Wales, tribunals are exempt from the operation of the *Privacy and Personal Information Protection Act 1998* (NSW) in respect of their judicial functions.[113] In Victoria and Tasmania, tribunals are exempt from state privacy legislation in respect of their judicial and quasi-judicial functions.[114] In the Northern Territory, tribunals are exempt from the operation of the *Information Act 2002* (NT) in relation to their decision-making functions.[115]

---

112 *Privacy Act 1988* (Cth) s 14 IPPs 10, 11; Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

113 *Privacy and Personal Information Protection Act 1998* (NSW) s 6(1).

114 *Information Privacy Act 2000* (Vic) s 10; *Personal Information Protection Act 2004* (Tas) s 7(a), (b).

115 *Information Act 2002* (NT) s 5(5)(a). A tribunal is defined as a body other than a court established by or under an Act that has judicial or quasi-judicial functions: *Information Act 2002* (NT) s 4.

Submissions and consultations

Industrial tribunals

32.78 In IP 31, the ALRC asked whether the AIRC, and the Industrial Registrar and Deputy Registrars should be exempt from the operation of the *Privacy Act*.[116] The President of the AIRC, the Hon Justice GM Giudice, submitted that the AIRC should remain exempt from the operation of the *Privacy Act* for two main reasons: the AIRC is obliged to act judicially; and, subject to some exceptions, its hearings and decisions are open to public scrutiny. His Honour stated that the policy issues that apply to the courts also apply to bodies that are required to act judicially, and therefore the AIRC should be in the same position as the courts.[117]

32.79 The Australian Government Department of Employment and Industrial Relations (DEWR) submitted that, on public interest grounds, the industrial tribunals should remain exempt in relation to non-administrative matters. DEWR suggested that:

> These organisations are not exempt in relation to their administrative activities, only in connection with their official functions. In this regard, these standard setting, conciliation and quasi-judicial tribunals are treated in the same fashion as federal courts … and DEWR is not aware of any compelling arguments to remove the exemption.[118]

32.80 While not commenting on whether the current partial exemptions that apply to industrial tribunals are appropriate, the OPC suggested that 'entities with like functions should be treated consistently under the *Privacy Act*'. The OPC also suggested that 'where exemptions apply it would be worthwhile introducing good privacy practices so that individuals understand how their personal information will be handled'.[119]

32.81 One individual submitted that there is no valid reason why there should be an exemption for agencies in the area of industry and workplace.[120]

Other federal tribunals

32.82 In IP 31, the ALRC asked whether any other federal tribunals should be exempt from the operation of the *Privacy Act*.[121] Other than the four federal tribunals that made submissions on this issue, the ALRC has received few responses to this question.[122] Of

---

116 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
117 Justice G Giudice, *Submission PR 91,* 15 January 2007.
118 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
119 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
120 K Handscombe, *Submission PR 89,* 15 January 2007.
121 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006) [5.69], Question 5–3.
122 The President of the AIRC also made a submission in relation to the current exemption from the operation of the *Privacy Act* that applies to the AIRC: Justice G Giudice, *Submission PR 91,* 15 January 2007 This issue is discussed in the following section.

the four tribunals—the AAT, MRT, RRT and SSAT—only the AAT submitted that it should be partially exempt from the operation of the *Privacy Act*.

Current legislative framework and application of the IPPs to federal tribunals

32.83 All four tribunals submitted that their legislative framework provides an appropriate level of safeguards for their handling of personal information, including requirements under different pieces of legislation,[123] and confidentiality obligations on tribunal staff prohibiting disclosure of information in particular circumstances.[124]

32.84 The tribunals also considered that the current exceptions to IPP 11 allow them to use personal information in the performance of their functions.[125] For example, the AAT submitted that:

> In disclosing personal information, the Tribunal generally relies on the following two exceptions to the basic rule set out in IPP 11 that personal information should not be disclosed:
>
> (a) individuals are reasonably likely to have been aware, or made aware, that the information is usually disclosed; and
>
> (d) the disclosure is required or authorised by law.

32.85 The AAT submitted, however, that:

> The precise scope of what the *Administrative Appeals Tribunal Act 1975* and the principle of open justice require or authorise in relation to the disclosure of information in the context of Tribunal proceedings is not entirely clear. [126]

32.86 The AAT also suggested that the application of IPP 7 in relation to its decisions may require consideration.

> The Tribunal recognises that, occasionally, there may be errors in relation to personal information recorded in decisions. The Administrative Appeals Tribunal Act 1975 provides for the alteration of the text of a decision in two circumstances:
>
> - where there is an obvious error in the text of a decision: s 43AA; and
> - where the Tribunal makes a confidentiality order in relation to certain information contained in the decision: s 35(2).
>
> Beyond these circumstances, however, the Tribunal does not alter the text of a decision that has been published.

---

123 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

124 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007.

125 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

126 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007.

> If it is alleged that an error in relation to the Tribunal's treatment of personal information amounts to an error of law, an appeal must be lodged in the Federal Court. There may be circumstances, however, in which the error is not relevant to the ultimate decision. It may be that a statement could be prepared which is appended to the decision. The precise circumstances in which this should occur and how it should be dealt with would need to be considered carefully.[127]

Openness of proceedings and decisions

32.87 Tribunals indicated in submissions that not all their proceedings are open to the public. The AAT and MRT are generally required by legislation to conduct hearings in public,[128] while the RRT and SSAT are required to conduct hearings in private.[129] The AAT submitted further that:

> it would be helpful in this context if the operation of the principle of open justice were given clearer expression in the legislative framework within which the Tribunal operates. Clarification of the Tribunal's powers in relation to the granting of access to documents and the publication of information would assist the Tribunal, parties, their representatives and the public to understand the way in which the Tribunal operates and exercises its powers.[130]

Exemptions for individual tribunals from the Privacy Act?

32.88 The AAT submitted that 'in the interests of consistency, it would be appropriate to treat the [AAT] in the same way as the federal courts'. In addition, the AAT stated that the principle of open justice applies to the AAT as it does to federal courts. It considered, however, that personal information about its personnel should continue to be dealt with in accordance with the *Privacy Act*.[131]

32.89 The MRT, RRT and SSAT submitted that they should not be exempt, either completely or partially, from the operation of the *Privacy Act*.[132] In a joint submission, the RRT and MRT submitted that they did not consider that there is a need for them to be exempt because IPP 11(1)(d) recognises adequately their need to disclose personal information for the purposes of their review functions. They stated that the provisions of their own governing legislation,

---

127 Ibid.
128 Ibid; Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007.
129 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
130 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007.
131 Ibid.
132 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

> in conjunction with the *Privacy Act*, operate effectively to ensure a balance between use and disclosure of personal information where required for review process and adequate protection of personal information.[133]

32.90 The SSAT did not consider that it should be exempt from the *Privacy Act*, provided that IPPs 10 and 11 remain essentially the same, so as to enable the use and disclosure of personal information by the SSAT.[134]

Exemption for 'federal tribunals' as a class of agencies from the Privacy Act?

32.91 The AAT and SSAT submitted that it may not be appropriate to exempt all federal tribunals.[135] The SSAT stated that agencies, and in particular, federal tribunals, should not be exempt from the operation of the *Privacy Act* by genus, particularly given the different objects and purposes of the FOI Act and *Privacy Act*. The SSAT submitted that:

> given the very diverse and particular natures of these tribunals' jurisdictions, the SSAT is of the view that a global response is not appropriate … It may be, in a particular case, that a particular tribunal, or particular acts or practices of a particular tribunal, should be exempt from the operation of the *Privacy Act*.[136]

32.92 Similarly, the AAT stated that exempting all federal tribunals from the *Privacy Act* in respect of their non-administrative activities may not be appropriate, because some of them are required to hold hearings in private.[137]

32.93 In contrast, the MRT and RRT stated that, although they do not consider that there is a need for them to be exempt from the operation of the *Privacy Act*, they anticipate that 'consideration may be given by the ALRC to the degree to which there should be consistency in coverage in respect to all federal tribunals'.[138]

32.94 The OPC noted that some tribunals, such as the AAT, have been the subject of complaints by individuals to the OPC.

> A number of the complaints have involved the AAT publishing its decisions. As with the exempt tribunals, the AAT has lawful authority to publish their findings … the Office would suggest that entities with like functions be treated consistently under the *Privacy Act*.[139]

---

133 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007.
134 Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
135 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
136 Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.
137 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007.
138 Migration Review Tribunal and Refugee Review Tribunal, *Submission PR 126,* 16 January 2007.
139 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

Exemption from the FOI Act

32.95 The AAT and SSAT submitted that they should be exempt from the FOI Act.[140] The AAT stated that it would be appropriate for it to be exempt from the FOI Act, in the same way as the courts, because

> access to documents relating to applications under the *[Administrative Appeals Tribunal] Act* should be dealt with in accordance with policies and practices developed by the Tribunal in the context of the operation of the principle of open justice, meeting the requirements of procedural fairness and providing appropriate protection of personal information.[141]

32.96 The SSAT submitted that it should be exempt from the FOI Act in respect of its review functions

> to ensure that persons are precluded from requesting access to documents provided to the SSAT for the purposes of carrying out its review function. Many of these documents arguably do not squarely come within the current FOI exemptions in Part IV of the FOI Act, and likewise may not be protected from disclosure by the confidentiality provisions in our own legislation. Given the sensitive and personal nature of our hearings … and the fact that the SSAT's hearings are legislatively required to be held 'in private', this seems to the SSAT to be desirable and appropriate.[142]

ALRC's view

32.97 The partial exemption of federal courts from the operation of the *Privacy Act* is based partly on the need to balance the principle of open justice with the interests of privacy. The principle of open justice, however, does not apply equally to all federal tribunals. The extent to which the principle applies to a particular tribunal depends on the nature of the tribunal's jurisdiction and the tribunal's operating environment. The principle of open justice also does not always apply equally to all proceedings before a particular tribunal. For example, some tribunals are generally required to hold hearings in public, but are required to hold particular types of hearings in private. They may also have a discretion as to whether to hold hearings in public or in private.

32.98 The partial exemption of federal courts is also based in part on the separation of powers in Chapter III of the *Australian Constitution*. This rationale does not apply to federal tribunals, which exercise executive rather than judicial power. Nevertheless, tribunals have adjudicative functions that are similar to the judicial functions of courts.[143] The functions of a tribunal generally include: evaluating evidence;

---

140 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007; Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

141 Administrative Appeals Tribunal, *Submission PR 201,* 20 February 2007.

142 Social Security Appeals Tribunal, *Submission PR 106,* 15 January 2007.

143 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005), [3.2.28]–[3.2.29].

conducting hearings; defining or determining any legal rights; and in the context of administrative review, not confining its evidence to that used by the decision maker.[144] On this basis, there is arguably a case for partially exempting federal tribunals from the *Privacy Act* in respect of their adjudicative functions.

32.99 Different tribunals are established, however, for different purposes. Some tribunals, such as the AAT, are generalist tribunals that adjudicate over a wide range of disputes. Other tribunals, such as the MRT and RRT, are specialist tribunals that hear a limited range of disputes. The jurisdictions of tribunals also differ in terms of the sensitivity of the subject matter. Some matters are particularly sensitive, such as the review of decisions by the RRT concerning protection visas for non-citizens.

32.100 To date, only two federal tribunals, the AAT and the AIRC, submitted that they should be exempt from the operation of the *Privacy Act*. Other federal tribunals that made submissions did not indicate that an exemption is necessary. The ALRC is interested in further views on whether federal tribunals should be exempt in respect of their adjudicative functions.

Exemption from the FOI Act

32.101 The AAT submitted that it should be exempt from the FOI Act in respect of non-administrative matters, on the basis that it is subject to the principle of open justice. The SSAT submitted that it should be exempt from that Act because of the sensitive and personal nature of its hearings, which are to be held in private.

32.102 IPPs 6 and 7 provide that the rights to access, or require the correction or amendment of, records held by agencies are subject to other applicable Commonwealth law, such as the FOI Act. Therefore, access and correction of records containing personal information about an individual are currently dealt with under the FOI Act. In Chapter 12, the ALRC proposes that an individual's right to access or correct his or her own personal information be dealt with in a new Part of the *Privacy Act* instead of under the FOI Act.[145]

32.103 It is beyond the ALRC's current Terms of Reference to inquire into access by persons other than the individual concerned to evidence and other documents produced in relation to tribunal proceedings under the FOI Act. Therefore, the ALRC does not propose to consider whether federal tribunals should be exempt from the operation of the FOI Act. As stated above, however, the ALRC reaffirms its recommendation in ALRC 98 that SCAG order a review of court and tribunal rules in relation to non-party access to court records, with a view to promoting a national and consistent policy.[146]

---

144 *Re Monger; Ex parte WMC Resources Pty Ltd* [2002] WASCA 129, [76].

145 Proposals 12–6, 12–7.

146 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 7–1.

32.104 As for an individual's right of access and correction in relation to his or her own personal information, the ALRC's preliminary view is that there may be some circumstances in which it is not appropriate for an individual to correct certain records, for example, written decisions by a federal tribunal. There may also be situations where access to a tribunal's records should not be granted because it might involve, for example, an unreasonable disclosure of personal information about another individual.

32.105 In Chapter 12, the ALRC invites submissions on what exceptions should apply to the general provision granting an individual the right to access his or her own personal information under the *Privacy Act*.[147] As part of that general question, the ALRC is interested in views on whether any exceptions should apply when granting an individual the right to access his or her own personal information held by a federal tribunal.

Question 32–1 Should the *Privacy Act* be amended to provide that federal tribunals are exempt from the operation of the Act in respect of their adjudicative functions? If so, what should be the scope of 'adjudicative functions'?

147 Question 12–1.

33. Exempt Agencies under the *Freedom of Information Act 1982* (Cth)

Contents

Introduction 955
Australian Fair Pay Commission 956
- Background 956
- Submissions and consultations 957
- ALRC's view 958

Schedule 2 Part I Division 1 of the *Freedom of Information Act* 959
- Background 959
- Aboriginal Land Councils and Land Trusts 960
- Auditor-General 960
- National Workplace Relations Consultative Council 961
- Submissions and consultations 962

Schedule 2 Part II Division 1 of the *Freedom of Information Act* 963
- Background 963
- Financial departments and agencies 963
- Australian Transaction Reports and Analysis Centre 964
- Media regulatory agencies 966
- National broadcasters 967
- Austrade 968
- National Health and Medical Research Council 968
- Submissions and consultations 969

ALRC's view 971

Introduction

33.1 Currently, a number of agencies are exempt from the requirements to comply with the *Privacy Act 1988* (Cth). The Act achieves this by reference to their exempt status under the *Freedom of Information Act 1982* (Cth) (FOI Act).[1] This chapter describes the functions of these agencies and considers whether they should remain exempt from the operation of the *Privacy Act*.

1 *Privacy Act 1988* (Cth) ss 7(1)(a)(i)(A)–(C), (b), (c). See also *Privacy Act 1988* (Cth) s 7A.

33.2 It should be noted that all Australian Government agencies, including the agencies discussed in this chapter, are required to comply with the *Protective Security Manual* (PSM 2005).[2] PSM 2005 is a policy document that sets out guidelines and minimum standards in relation to protective security for agencies and officers, as well as for contractors and their employees who perform services for the Australian Government. In particular, Part C of the PSM 2005 provides 'guidance on the classification system and the protective standards required to protect both electronic- and paper-based security classified information'.[3] This part sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

33.3 Australian Government agencies are also required by the PSM 2005 to comply with the *Australian Government Information Technology Security Manual* (ACSI 33). ACSI 33 has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on the protection of their electronic information system.[4]

33.4 Although the PSM 2005 addresses some privacy issues that are dealt with under the Information Privacy Principles (IPPs) of the *Privacy Act*, the privacy protection under the PSM 2005 guidelines is restricted to security classified information and does not deal with other matters under the IPPs, such as the accuracy of personal information.

Australian Fair Pay Commission

Background

33.5 Section s 7(1) of the *Privacy Act* provides that an agency listed in Schedule 1 of the FOI Act is exempt from the operation of the *Privacy Act*, except in respect of matters of an administrative nature.[5] One of the agencies listed under Schedule 1 of the FOI Act is the Australian Fair Pay Commission (AFPC). The other agencies listed in Schedule 1 of the FOI Act are the Australian Industrial Relations Commission (AIRC), and the Industrial Registrar and Deputy Registrars. The exemption that applies to these other agencies is considered in Chapter 32.

33.6 Section 7(1) was originally intended to exempt from the operation of the *Privacy Act* 'industrial tribunals referred to in Schedule 1 of the FOI Act in respect of

---

2 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 31 July 2007.

3 Ibid.

4 Defence Signals Directorate, *Australian Government Information Technology Security Manual (ACSI 33)* (2004). There are two versions of ACSI 33. The security-in-confidence version contains the security policies and guidance for all classifications. The unclassified version only contains policies and guidance for the following classifications: public domain·unclassified, in-confidence, restricted, and protected. An unclassified version of ACSI 33 is available on the DSD's website: Defence Signals Directorate, *Australian Government Information Technology Security Manual (ACSI 33)* (2004).

5 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(A), (b).

administrative matters',[6] such as the Australian Conciliation and Arbitration Commission (now the AIRC), and the Industrial Registrar and Deputy Industrial Registrars. In 2006, the FOI Act, which provides the mechanism for this exemption from the operation of the *Privacy Act*, was amended to include the AFPC in Schedule 1 of that Act.[7] The secondary materials relating to the regulations do not disclose the policy behind the exemption of the AFPC from the FOI Act and the *Privacy Act*.

33.7 The AFPC is an independent, statutory body established under the *Workplace Relations Amendment (WorkChoices) Act 2005* (Cth). The AFPC is responsible for setting and adjusting federal minimum wages to promote the economic prosperity of the people of Australia. The AFPC took over the wage-setting and adjusting functions of the AIRC, which retains its role as a national industrial tribunal dealing with employment disputes.[8] The primary functions of the AFPC are to conduct wage review and exercise its wage-setting powers as necessary. The main wage-setting powers of the AFPC include adjusting the standard federal minimum wage, as well as determining and adjusting: minimum classification rates of pay; special federal minimum wages for junior employees, employees with disabilities or employees to whom training arrangements apply; basic periodic rates of pay and basic piece rates of pay payable to employees or employees of particular classifications; and casual loadings.[9]

33.8 In performing its wage-setting function, the AFPC may inform itself in any way it thinks appropriate, including by: undertaking or commissioning research; consulting with any other person, body or organisation; or monitoring and evaluating the impact of its wage-setting decisions.[10] The AFPC must publish written wage-setting decisions and include reasons in its decisions.[11]

Submissions and consultations

33.9 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether agencies specified in Schedule 1 of the FOI Act, including the Australian Fair Pay Commission, should be exempt from the *Privacy Act*.[12]

33.10 Few stakeholders commented specifically on the exemption that applies to the AFPC. The Australian Government Department of Employment and Industrial Relations (DEWR) submitted that the partial exemption that applies to agencies

---

6 Explanatory Memorandum, Privacy Bill 1988 (Cth), [45].

7 *Workplace Relations Amendment (Work Choices) (Consequential Amendments) Regulations* (No. 1) *2006* (Cth) sch 36.

8 Australian Fair Pay Commission, *About the Commission* <www.fairpay.gov.au/fairpay/About> at 4 August 2007; *Workplace Relations Act 1996* (Cth) s 23.

9 *Workplace Relations Act 1996* (Cth) s 22(1).

10 Ibid ss 24(2).

11 Ibid ss 24(4), 26(1).

12 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.

specified under Schedule 1 of the FOI Act should remain, because agencies that exercise standard-setting, conciliation and quasi-judicial functions should be exempt to the same extent as federal courts. It stated that it was not aware of any compelling arguments to remove the exemption.[13] In contrast, one individual submitted that there is no valid reason why agencies that deal with workplace and employment issues should be exempt.[14]

33.11 While the Office of the Privacy Commissioner (OPC) did not comment on whether the AFPC should remain exempt, it stated that 'entities with like functions should be treated consistently under the *Privacy Act*'. The OPC also suggested that 'where exemptions apply it would be worthwhile introducing good privacy practices so that individuals understand how their personal information will be handled'.[15]

33.12 More generally, some stakeholders submitted that exemptions of agencies from the operation of the *Privacy Act*, including those specified in the FOI Act, should be limited to the extent possible and any exemption should be justified.[16] The Commonwealth Ombudsman suggested that, 'even where an agency is exempt from coverage by the *Privacy Act*, it should be encouraged to adopt similar standards to the extent possible'.[17]

33.13 It was suggested in one submission that there is no justification for such broad exemptions from the *Privacy Act* for any of the agencies specified in Schedule 1 of the FOI Act.

> Any difficulties that compliance with the privacy principles might cause them should be dealt with by means of selective exceptions to particular principles and provisions, but only on the basis of detailed justification … The extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the *Act*.[18]

ALRC's view

33.14 The original exemption under the *Privacy Act* was intended to apply to industrial tribunals, such as the AIRC. Since the AFPC has only taken over the AIRC's wage-setting function and not its dispute resolution function, the original policy justification that applied to industrial tribunals does not apply to the AFPC. Further, there appears to be no stated policy reason for exempting the AFPC from the requirement to comply with the *Privacy Act* in respect of its non-administrative functions. Therefore, it would appear that this exemption of the AFPC from the

---

13 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
14 K Handscombe, *Submission PR 89,* 15 January 2007.
15 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
16 See, eg, Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
17 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.
18 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

Privacy Act only applies by virtue of the fact that the AFPC is now listed in Schedule 1 of the FOI Act.

33.15 As discussed in Chapter 30, any exemption from the *Privacy Act* should be limited to the extent possible and justified on sound policy grounds. There does not appear to be any policy justification for the AFPC's exemption. The function of standard setting cannot be compared with the exercise of judicial power, which is conferred by the *Australian Constitution*; or dispute resolution, where there may be an argument that the *Privacy Act* presents barriers to information exchange that is necessary for effective and efficient dispute resolution. The ALRC, therefore, proposes that the exemption that applies to the AFPC be removed.

33.16 Currently, the AFPC is exempt from provisions in the FOI Act, which grant an individual the right to access the AFPC's documents unless those documents relate to matters of an administrative nature.[19] In Chapter 12, the ALRC proposes that an individual's right to access or correct his or her own personal information be dealt with in a new Part of the *Privacy Act* instead of under the FOI Act.[20] The ALRC is also inviting submissions on what exceptions should apply to the general provision granting an individual the right to access his or her own personal information.[21] As part of that general question, the ALRC is interested in views on whether the AFPC should continue to be exempt from the general provision granting an individual the right to access his or her own personal information.

Proposal 33–1 The *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Fair Pay Commission under s 7(1) of the Act.

Schedule 2 Part I Division 1 of the *Freedom of Information Act*

Background

33.17 Certain agencies listed in Schedule 2 Part I Division 1 of the FOI Act—including Aboriginal Land Councils and Land Trusts,[22] the Auditor-General and the National Workplace Relations Consultative Council—are exempt from compliance

19 *Freedom of Information Act 1982* (Cth) s 6.
20 Proposals 12–6, 12–7.
21 Question 12–1.
22 Aboriginal Land Councils and Land Trusts are created under the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth).

with the IPPs.[23] Other provisions of the Act, such as the tax file number provisions do apply to these agencies.

33.18 Section 7A of the *Privacy Act* provides that agencies listed in Schedule 2 Part I of the FOI Act should be treated as organisations, if prescribed by regulation. Where an agency has been prescribed by regulation for this purpose, the National Privacy Principles (NPPs) or an approved privacy code will apply. Currently, the only prescribed agencies are the Australian Government Solicitor and the Australian Industry Development Corporation.[24]

Aboriginal Land Councils and Land Trusts

33.19 Aboriginal Land Councils and Land Trusts were exempted from the FOI Act because they are separate from the executive arm of the government and therefore not subject to public sector responsibilities.[25] It is likely that this is also the reason that these bodies were exempted from the *Privacy Act* when that Act applied only to the public sector. It is unclear why they remain exempt from the *Privacy Act* now that the Act has been extended to the private sector.

Auditor-General

33.20 The Auditor-General is an independent statutory officer responsible for auditing the activities of most Commonwealth public sector entities. The Auditor-General is supported by the Australian National Audit Office, which provides the Australian Parliament with an independent assessment of certain areas of public administration, and assurance about public sector financial reporting, administration and accountability. The Auditor-General has broad information-gathering powers and authority to have access to Commonwealth premises.[26] While the Auditor-General is not required to comply with the IPPs, s 36(1) of the *Auditor-General Act 1997* (Cth) provides that a person who has obtained information in the course of performing an Auditor-General function must not disclose that information except in the course of performing that function.[27]

---

23 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2). The intelligence agencies—namely, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service and the Office of National Assessment—and the Inspector-General of Intelligence and Security are also listed in sch 2 pt I div 1 of the FOI Act. Issues concerning the exemption of these agencies from compliance with the *Privacy Act* are discussed in Ch 31.

24 *Privacy (Private Sector) Regulations 2001* (Cth) reg 4. Note that the *AIDC Sale Act 1997* (Cth) provides for the sale of AIDC Ltd, the main operating subsidiary of the Australian Industry Development Corporation, and the progressive winding-down of the Australian Industry Development Corporation. AIDC Ltd was sold in 1998: Commonwealth of Australia, *Commonwealth National Competition Policy—Annual Report 1997–98* (1999). Due to some long term obligations, however, the winding down of the Australian Industry Development Corporation is unlikely to be completed before 2010: Australian Industry Development Corporation, *Statement of Intent* <www.finance.gov.au/gbab/docs/AIDC_SOI.pdf> at 16 August 2007.

25 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

26 *Auditor-General Act 1997* (Cth) pt 5 div 1.

27 Ibid s 36.

National Workplace Relations Consultative Council

33.21 The National Workplace Relations Consultative Council is a consultative body that provides a forum for representatives of the Australian Government, employers and employees to discuss workplace relations matters of national concern.[28] In its review of the Freedom of Information Bill 1978 (Cth), the Senate Standing Committee on Constitutional and Legal Affairs expressed the view that the Council should not be exempt from the FOI legislation because the Council was a consultative body rather than an industrial tribunal, and the Council's proceedings were adequately protected under another provision of the Bill.[29]

33.22 During parliamentary debate on the Freedom of Information Bill 1981 (Cth), a number of parliamentarians commented that there was no reasonable justification for exempting many of the agencies in Schedule 2 to the Bill, many of which did not have commercial or intelligence functions.[30] Particular mention was made of the Aboriginal Land Councils and Land Trusts, the Auditor-General and the National Labour Consultative Council.[31]

33.23 In their 1994 inquiry into the FOI Act, the ALRC and the Administrative Review Council (ARC) commented that decisions to exempt particular agencies from the FOI Act have tended to be selective.[32] The ALRC and ARC recommended that all agencies listed in Schedule 2 Part I of the FOI Act (other than the intelligence agencies, the Inspector-General of Intelligence and Security and government business enterprises) should be required to demonstrate to the Attorney-General the grounds on

---

28 *National Workplace Relations Consultative Council Act 2002* (Cth) s 5.

29 Parliament of Australia—Senate Standing Committee on Constitutional and Legal Affairs, *Freedom of Information—Report by the Senate Standing Committee on Constitutional and Legal Affairs on the Freedom of Information Bill 1978, and Aspects of the Archives Bill 1978* (1979), [12.36].

30 Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 44 (L Bowen), 47–48; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 49 (I Harris), 50–51; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 428 (B Jones), 430–431; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 439 (D Cameron), 439–440; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 440 (P Milton), 441; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 379 (A Theophanous), 381; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 388 (J Carlton), 389–390; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 391 (B Howe), 393.

31 Commonwealth, *Parliamentary Debates*, House of Representatives, 18 August 1981, 49 (I Harris), 51; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 439 (D Cameron), 439–440; Commonwealth, *Parliamentary Debates*, House of Representatives, 19 August 1981, 440 (P Milton), 441; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 379 (A Theophanous), 381; Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 1982, 391 (B Howe), 393.

32 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

which they should be exempt from the operation of that Act. If they did not do this within 12 months, they should be removed from Schedule 2 Part I of that Act.[33]

33.24 On 5 September 2000, the Freedom of Information Amendment (Open Government) Bill 2000 (Cth) was introduced into the Senate by Senator Andrew Murray as a Private Member's Bill. The Bill was designed to amend the FOI Act to give effect to recommendations made by the ALRC and ARC. One proposal under the Bill was to revoke the exempt status of many of the agencies and particular documents of certain agencies listed in Schedule 2 to the FOI Act.[34]

33.25 The provisions of the Bill were referred to the Senate Legal and Constitutional Legislation Committee for inquiry. In its report, the Committee did not support the proposal to remove the exempt status from these agencies and documents on the basis that alternative ways of structuring the exemption provisions under the FOI Act should be examined more closely before amending the legislation.[35] The Bill was amended to remove the proposal.[36]

Submissions and consultations

33.26 In IP 31, the ALRC asked whether agencies specified in Schedule 2 Part I Division 1 of the FOI Act should be exempt from the *Privacy Act*.[37]

33.27 The ALRC received few submissions that commented specifically on this question. As mentioned above, some stakeholders submitted that the general approach to the exemption of any agencies from the *Privacy Act*, including those specified in the FOI Act, is that: the exemption should be limited to the extent possible and justified;[38] any exempt agency should be encouraged to adopt standards similar to those under the *Privacy Act* to the extent possible;[39] and any difficulties that compliance with the privacy principles might cause such agencies should be dealt with by means of selective exceptions on the basis of detailed justification.[40]

33.28 The Queensland Council for Civil Liberties submitted that where exemptions are justified, they should take the form of exceptions to the privacy principles. It submitted that, on this basis, agencies specified in Schedule 2 of the FOI Act

---

33 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 74.

34 See Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [1.1]–[1.2], [3.31].

35 Ibid, [3.137].

36 The Bill lapsed due to the Australian Parliament being prorogued on 31 August 2004. It was reintroduced as the Freedom of Information Amendment (Open Government) Bill 2003 [2004] (Cth) and is currently before the Senate.

37 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.

38 See, eg, Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

39 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.

40 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

> should be required to demonstrate why they need to be exempt from the *Privacy Act* and if they do not do so, within a specified period of time, they should no longer be exempt. This follows from our generally accepted principle that privacy principles should apply universally unless there is some demonstrated reason why they should not be.[41]

Schedule 2 Part II Division 1 of the *Freedom of Information Act*

Background

33.29 A number of agencies listed in Schedule 2 Part II Division 1 of the FOI Act are exempt from the *Privacy Act* where their acts and practices relate to documents specified in the FOI Act, to the extent that those documents relate to the non-commercial activities of the agencies or of other entities.[42] In relation to documents that are *not* specified under the FOI Act, these agencies are covered by the IPPs where the documents concern the agencies' non-commercial activities or the non-commercial activities of other entities.[43] These agencies are also covered by the NPPs where their acts and practices relate to commercial activities or to documents concerning commercial activities.[44] In addition, they are required to comply with the tax file number provisions and, where applicable, the credit reporting provisions of the *Privacy Act*.[45] These agencies are described below.

Financial departments and agencies

33.30 The Australian Government Department of the Treasury focuses primarily on economic policy and has four principal functions—fostering a sound macroeconomic environment, advising on effective government spending and taxation arrangements, assisting in the formulation and implementation of effective taxation and retirement income arrangements, and advising on policy process and reforms that promote well functioning markets.[46] The Department's acts and practices relating to documents concerning the activities of the Australian Loan Council are exempt from the IPPs and NPPs to the extent that those documents relate to non-commercial activities.[47]

33.31 The Reserve Bank of Australia is a statutory authority, responsible for: formulating and implementing monetary and banking policy; maintaining financial

---

41 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. A similar view was expressed by K Handscombe, *Submission PR 89,* 15 January 2007.

42 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

43 Ibid s 7(1)(c).

44 Ibid s 7A.

45 Ibid s 7(2).

46 Australian Government—The Treasury, *About Treasury* <www.treasury.gov.au> at 11 August 2007.

47 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A. The Australian Loan Council is a Commonwealth-State ministerial council that coordinates public sector borrowing. It comprises of the Australian Government Treasurer as Chairman, and state and territory treasurers: Australian Government, *2005–06 Budget Paper No 3—Federal Financial Relations 2005–06* (2005), 36.

system stability; contributing to the maintenance of full employment in Australia; and promoting the safety and efficiency of the payments system. It actively participates in financial markets, manages Australia's foreign reserves, issues Australian currency notes and serves as banker to the Australian Government.[48] The Reserve Bank has power to: receive money on deposit; borrow and lend money; buy, sell, discount and re-discount bills of exchange, promissory notes and treasury bills; buy and sell securities issued by the Australian Government and other securities; buy, sell and otherwise deal in foreign currency, specie, gold and other precious metals; establish credits and give guarantees; issue bills and drafts and effect transfers of money; underwrite loans; and issue, re-issue or cancel Australian notes.[49] The Reserve Bank is exempt where its acts and practices relate to documents concerning its banking operations (including individual open market operations and foreign exchange dealings) or exchange control matters, to the extent that these documents relate to non-commercial activities.[50]

33.32 The Export and Finance Insurance Corporation is a self-funding statutory corporation wholly owned by the Australian Government. It provides competitive finance and insurance services to Australian exporters and Australian companies investing in new projects overseas.[51] The Corporation is exempt from the operation of the *Privacy Act* where its acts and practices relate to documents concerning anything it has done under Part 4 (insurance and financial services and products) or Part 5 (national interest transactions) of the *Export Finance and Insurance Corporation Act 1991* (Cth), to the extent that those documents relate to non-commercial activities.[52]

Australian Transaction Reports and Analysis Centre

33.33 The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit within the portfolio of the Attorney-General. It oversees compliance with the reporting requirements of the *Financial Transaction Reports Act 1988* (Cth) and *Anti-Money Laundering and Counter-terrorism Financing Act 2006* (Cth) (AML/CTF Act) by a wide range of financial services providers, the gambling industry and others. It also provides financial transaction report information to state, territory and Australian law enforcement, security, social justice and revenue agencies, as well as certain international counterparts.[53] AUSTRAC is exempt from compliance with the *Privacy Act* in respect of documents concerning information communicated to it in relation to:

---

48 Reserve Bank of Australia, *About the RBA* <www.rba.gov.au/AboutTheRBA/> at 10 August 2007. See also *Reserve Bank Act 1959* (Cth) s 10.

49 *Reserve Bank Act 1959* (Cth) ss 8, 34.

50 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

51 Australian Government Export and Finance Insurance Corporation, *About Us* <www.efic.gov.au> at 10 August 2007.

52 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

53 AUSTRAC, *About AUSTRAC* <www.austrac.gov.au> at 10 August 2007.

- reports of suspected illegal transactions by cash dealers involving currency in excess of $10,000 under s 16 of the *Financial Transaction Reports Act*; [54]

- reports of suspicious matters—that is, the reporting of a matter where there are reasonable grounds to suspect that funds are the proceeds of criminal activity, or are related to terrorism financing or money laundering—under s 41 of the AML/CTF Act; and

- further information requested by AUSTRAC from a reporting entity in relation to reports of suspicious matters, threshold transactions[55] and certain international funds transfer transactions under s 49 of the AML/CTF Act.[56]

33.34 Part 11 of the AML/CTF Act contains secrecy and access provisions concerning information obtained or held by AUSTRAC. Section 123 of the AML/CTF Act creates offences for 'tipping off'. A reporting entity is prohibited from disclosing that it has: formed a suspicion about a transaction or matter; given, or is required to give, a suspicious matter report to AUSTRAC; or provided further information under s 49(1) of the AML/CTF Act.[57] A similar provision in the *Financial Transaction Reports Act* applies to cash dealers in relation to suspected illegal transactions.[58]

33.35 An AUSTRAC official is prohibited from disclosing information or documents collected, compiled or analysed by AUSTRAC except for the purposes of: the Act; the performance of the functions of the Chief Executive Officer of AUSTRAC (AUSTRAC CEO); or the performance of the official's duties under the AML/CTL Act or the *Financial Transaction Reports Act*.[59] In addition, AUSTRAC officials and other investigating officials (such as the Commissioner of the Australian Federal Police and the Chief Executive Officer of the Australian Crime Commission) are prohibited from disclosing any information obtained under s 49 of the AML/CTL Act except for the purposes of the Act or in connection with their official functions and duties.[60]

---

54 A 'cash dealer' is defined to include, for example, a financial institution, an insurer or an insurance intermediary, a person who carries on a business of collecting, holding, exchanging, remitting or transferring currency on behalf of other persons: *Financial Transaction Reports Act 1988* (Cth) s 3.

55 A 'threshold transaction' means a transaction involving the transfer of not less than $10,000 of physical currency or e-currency, or a transaction specified in regulations to be a threshold transaction: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5.

56 *Privacy Act 1988* (Cth) s 7(1)(c). A reporting entity is a person who provides a 'designated service': *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 5. Designated services include a wide range of specified financial services, bullion trading services, gambling services and other prescribed services: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 6.

57 This is subject to certain exceptions under s 123(4)–(8) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

58 *Financial Transaction Reports Act 1988* (Cth) s 16(5A), (5AA).

59 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 121.

60 Ibid s 122.

33.36 In the performance of his or her functions, the AUSTRAC CEO must consult with the Privacy Commissioner and take into account his or her comments made in the course of those consultations.[61]

33.37 The interaction between the AML/CTF Act and the *Privacy Act* is discussed further in Chapter 13.

Media regulatory agencies

33.38 The Australian Communications and Media Authority (ACMA) is a statutory body responsible for the regulation of broadcasting, radiocommunications, telecommunications and the internet. Its responsibilities include: promoting self-regulation and competition in the communications industry, while protecting consumers and other users; fostering an environment in which electronic media respects community standards and responds to audience and user needs; managing access to the radiofrequency spectrum; and representing Australia's communications and broadcasting interests internationally.[62]

33.39 The Classification Board and the Classification Review Board are separate and independent statutory bodies. The Classification Board classifies films (including videos and DVDs), computer games and certain publications before they are made available to the public. It also provides classifications to ACMA on internet content, advice to enforcement agencies such as the police, and advice to the Australian Customs Service.[63] The Classification Review Board is a part-time body that reviews the classification of films, publications or computer games upon receipt of a valid application to review the decisions of the Classification Board.[64]

33.40 The Office of Film and Literature Classification was an agency within the Attorney-General's portfolio that provided support to the Classification Board and the Classification Review Board. On 1 July 2007, the Attorney-General's Department took over the policy and administrative functions of the Office of Film and Literature Classification and the Office ceased to exist as a separate agency.[65]

33.41 The Classification Board, the Classification Review Board and the Attorney-General's Department are exempt from the *Privacy Act* where their acts and practices concern 'exempt Internet-content documents' under Schedule 5 to the *Broadcasting*

---

61 Ibid s 212(2).

62 Australian Communications and Media Authority, *About ACMAs Role* <www.acma.gov.au> at 10 August 2007.

63 Australian Government Office of Film and Literature Classification, *The Classification Board* <www.classification.gov.au> at 6 August 2007.

64 Australian Government Office of Film and Literature Classification, *The Classification Review Board* <www.classification.gov.au> at 6 August 2007.

65 Australian Government Attorney-General's Department, *Administrative Arrangements for the Classification Board and Classification Review Board* <www.ag.gov.au/www/agd/agd.nsf/Page/RWPEB9317B18576C244CA2572D700023C62> at 6 August 2007.

Services Act 1992 (Cth).[66] An 'exempt Internet-content document' is a document containing offensive information that has been copied from the internet; or a document that sets out how to access, or is likely to facilitate access to, offensive information on the internet.[67]

National broadcasters

33.42 The Australian Broadcasting Corporation (ABC) is a statutory corporation and Australia's only national, non-commercial broadcaster. The Special Broadcasting Service (SBS) is Australia's multicultural and multilingual public broadcaster. It was established under the *Special Broadcasting Services Act 1991* (Cth) to provide multilingual and multicultural radio and television services.[68]

33.43 Pursuant to s 7(1)(c) of the *Privacy Act*, both the ABC and SBS are covered by the *Privacy Act* except in relation to their program materials[69] and datacasting content.[70] Section 7A of the Act provides, however, that despite s 7(1)(c), certain acts and practices of the agencies listed in Schedule 2 Part II Division 1 of the FOI Act (which includes the ABC and SBS) are to be treated as acts and practices of organisations. These include acts and practices in relation to documents concerning their commercial activities or the commercial activities of another entity, and acts and practices that relate to those commercial activities.[71] Therefore, it would appear that, apart from their program materials and datacasting content, the ABC and SBS are covered by the IPPs in relation to non-commercial activities, and the NPPs in relation to commercial activities. To the extent that their program materials and datacasting content relate to commercial activities, they are covered by the private sector provisions of the *Privacy Act*.

---

66 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

67 *Freedom of Information Act 1982* (Cth) s 4(1).

68 *Special Broadcasting Service Act 1991* (Cth) s 6.

69 In *Rivera v Australian Broadcasting Corporation* (2005) 222 ALR 189, Hill J of the Federal Court of Australia held that s 7(1)(c) of the *Privacy Act* operated so as to exempt any acts and practices of the ABC dealing with records concerning its program material and therefore the court had no jurisdiction to grant relief under the Act. One commentator observed that the court's attention had not been drawn to all the relevant provisions of the Act, including the media exemption and s 7A which provides that *despite* s 7(1)(c), the ABC is subject to the NPPs where its acts and practices concerns commercial activities: P Gunning, 'Cases + Complaints: Rivera v Australian Broadcasting Corporation [2005] FCA 661' (2004) 11 *Privacy Law & Policy Reporter* 205. In *Australian Broadcasting Corporation v The University of Technology, Sydney* (2006) 91 ALD 514, Bennett J of the Federal Court of Australia held that the ABC is exempt under the *Freedom of Information Act 1982* (Cth) in relation to documents that have a direct or indirect relationship to ABC's program materials, provided that those documents also have a relationship to the ABC.

70 'Datacast' means to broadcast digital information: *Macquarie Dictionary* (online ed, 2005). Under s 6 of the *Broadcasting Services Act 1992* (Cth), 'datacasting service' means a service that delivers content using the broadcasting services bands—whether in the form of text; data; speech, music or other sounds; visual images; or any other form—to persons with the appropriate equipment for receiving that content.

71 *Privacy Act 1988* (Cth) s 7A.

33.44 The relevant Revised Explanatory Memorandum stated, however, that s 7A was not intended to apply to the ABC and SBS.

> The effect of new clause 7A is to make the acts and practices of some agencies subject to the standards in the NPPs (or an approved privacy code, as appropriate), to the extent that they are not currently subject to the Information Privacy Principles (by virtue of section 7 of the Act). The Government's policy is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the NPPs, just like private sector organisations …
>
> The aim of the amendment is to ensure that an agency in Division 1 of Part II of Schedule 2 to the FOI Act complies with the standards set out in the NPPs or an approved privacy code (as appropriate) in relation to documents in respect of its commercial activities or the commercial activities of another entity. This clause is intended to apply to agencies such as Comcare, the Health Insurance Commission and Telstra Corporation Limited. It is not intended to apply to the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.[72]

33.45 Where the acts and practices of the ABC and SBS are to be treated as those of organisations, they may still be exempt if carried out in the course of journalism.[73] The media exemption relating to journalism is discussed in Chapter 38.

Austrade

33.46 The Australian Trade Commission (Austrade) was established by the *Australian Trade Commission Act 1985* (Cth). Its functions are to provide advice, market intelligence and support to Australian companies to reduce the time, cost and risk involved in selecting, entering and developing international markets. In addition, it provides advice and guidance on overseas investment and joint venture opportunities. Austrade also administers the Export Market Development Grants scheme, which provides financial assistance to eligible businesses through partial reimbursement of the costs of specified export promotion activities.[74]

33.47 Austrade is exempt from the operation of the *Privacy Act* where its acts and practices relate to documents concerning the carrying out of overseas development projects, to the extent that these documents relate to non-commercial activities.[75]

National Health and Medical Research Council

33.48 The National Health and Medical Research Council (NHMRC) is a statutory agency responsible for promoting the development and maintenance of public and individual health standards. It does this by fostering the development of consistent

---

72 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [102], [104].

73 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

74 Austrade, *What is Austrade?* <www.austrade.gov.au> at 10 August 2007.

75 An overseas development project is a project to be carried out in a foreign country by way of: the construction of works; the provision of services; the design, supply or installation of equipment or facilities; or the testing in the field of agricultural practices: *Australian Trade Commission Act 1985* (Cth) s 3(1).

health standards between the various states and territories, fostering health and medical research and training, and monitoring ethical issues relating to health throughout Australia.[76]

33.49 The NHMRC is exempt from the *Privacy Act* where its acts and practices relate to documents in the possession of its Council members who are not persons appointed or engaged under the *Public Service Act 1999* (Cth), to the extent that these documents relate to non-commercial activities.

Submissions and consultations

33.50 In IP 31, the ALRC asked whether agencies specified in Schedule 2 Part II Division 1 of the FOI Act—other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation—should be exempt from the *Privacy Act*.[77] The ALRC received few submissions that commented specifically on the exemption of these agencies.

33.51 A concern was raised in one submission about the large number of agencies listed under Schedule 2 Part II Division 1 of the FOI Act that are exempt both from the FOI Act and the *Privacy Act*. It was submitted that only those exemptions that are necessary for national security or to curb criminal activity are justified.[78]

33.52 AUSTRAC submitted that its partial exemption from the *Privacy Act* should remain. It suggested that there are two important policy reasons behind the exemption concerning the reporting of suspected illegal transactions: first, individuals should not be alerted to the fact that suspect transaction reports were made in relation to them because

> such reports may be relevant to criminal investigations or investigation relating to terrorism financing and tipping off may prejudice those investigations. In addition, cash dealer staff members that report such transactions may be put at risk if it is disclosed that a suspect transaction report has been lodged.[79]

33.53 AUSTRAC stated that cash dealers have legitimate concerns about protecting their staff from retribution for filing a suspected transaction report. It submitted that if information concerning the existence of a suspected transaction report could become known to the subject of the report, there would be a decrease in both the number and quality of suspected transaction reports.[80]

---

76 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 1 August 2007.
77 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
78 K Handscombe, *Submission PR 89,* 15 January 2007.
79 AUSTRAC, *Submission PR 216,* 1 March 2007.
80 Ibid.

33.54 AUSTRAC submitted further that 'protecting the privacy of AUSTRAC's information is a key priority for the agency'. It submitted that there is a high level of privacy protection in relation to AUSTRAC's information, including: training for all staff on privacy requirements; secrecy and access provisions under Part 11 of the AML/CTF Act; limited access to AUSTRAC information pursuant to an Instrument of Authorisation signed by the AUSTRAC CEO under s126(1) of the AML/CTF Act; Memoranda of Understanding between the AUSTRAC CEO and the Chief Executive of 29 of the 33 designated agencies that are entitled or authorised to have access to AUSTRAC information; audit trails of access to suspected transactions reports by its own staff, the Australian Taxation Office and designated agency officers; and a legislative requirement that, in the performance of his or her functions, the AUSTRAC CEO consult with the Privacy Commissioner.[81]

33.55 The ABC submitted that the exemptions applying to agencies listed in Schedule 2 Part II Division 1 of the FOI Act should remain, on the basis that:

> the current scheme of exemptions applying to Part II Division 1 Agencies, whereby those agencies are exempted from the IPPs in respect of certain acts or practices, but are then subject to the NPPs as if they were an organisation, strikes the right balance in maintaining a level playing field between those public sector organisations and private sector organisation with which they may be in competition.[82]

33.56 The ABC and SBS submitted that they should continue to be exempt from the *Privacy Act* in respect of their programming materials and datacasting contents.[83] Both stated that their programming materials and datacasting content are not commercial activities and are therefore not covered by the NPPs. The ABC further suggested that s 7A of the Act, which requires that certain agencies comply with the NPPs in relation to their commercial activities, was not intended to apply to the ABC in relation to any of its activities. The ABC submitted that this suggestion is evident from the Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth), and that it also is

> supported by the *Australian Broadcasting Corporation Act 1983* (Cth) … under which the ABC is an independent authority with a particular charter broadcasting functions that are quite readily distinguishable from the imperatives of the commercial broadcasting sector …
>
> The charter functions of the national broadcasters, and the fact that they are subject to governance requirements very different from those applying to private sector media organisations, suggest that they should not be regarded as being in commercial competition with those entities. This argument arguably is stronger in relation to the ABC, which is required by the ABC Act not to broadcast advertisements (section 31 [of the *Australian Broadcasting Corporation Act*]).[84]

---

81 Ibid.

82 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

83 SBS, *Submission PR 112,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

84 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

33.57 SBS, on the other hand, suggested that it is covered by s 7A of the *Privacy Act* to the extent that it engages in commercial activities. SBS submitted that the policy concern behind s 7A—that agencies operating in the commercial sphere should operate on a level playing field with organisations—is applicable to the SBS. It stated:

> The partial exemption in relation to 'commercial activities' should be retained, so that 'hybrid' organisations such as SBS and the ABC which are government organisations which undertake some activities of a commercial nature, are not disadvantaged by being required to disclose information about their commercial activity.[85]

33.58 The ABC and SBS submitted that being exempt from the operation of the IPPs and NPPs in relation to their program-making activities does not mean that they are not subject to privacy regulation or oversight. They observed that they are subject to privacy provisions in their editorial policies, as well as codes of practice that must be notified to ACMA, which investigates complaints about alleged breaches of the codes.[86]

ALRC's view

33.59 The exemption of the agencies listed under Schedule 2 of the FOI Act from the *Privacy Act* is expressed in terms of their exemption from the FOI Act. Therefore, their exemption from the operation of the *Privacy Act* derives from their status under the FOI Act. The purposes of the *Privacy Act* are, however, different from those of the FOI Act. The *Privacy Act* is mainly concerned with the protection of the privacy of personal information about individuals, whereas the FOI Act aims to promote the ideals of an open and transparent government by granting a right of access to, and correction of, government records, except in relation to certain exempt documents. Given the differing purposes of the two Acts, the ALRC questions whether simply adopting the exemption in the FOI Act is appropriate. In the ALRC's view, there should be clear policy justifications for the exemption of these agencies from the *Privacy Act*.

33.60 Except for the ABC, SBS and AUSTRAC, the ALRC has not received submissions from the exempt agencies about their exemption from the operation of the *Privacy Act*, despite specifically inviting submissions from them.[87] Given the lack of information, the ALRC is unable to make an informed policy decision on a number of these agencies specified in Schedule 2 Part I Division 1 and Part II Division 1 of the

---

85 SBS, *Submission PR 112,* 15 January 2007.

86 Ibid; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

87 In October 2006, the ALRC wrote to the following agencies inviting submissions: Anindilyakwa Land Council, Tiwi Land Council, Northern Land Council, Central Land Council, Auditor-General of Australia, National Workplace Relations Consultative Council, Reserve Bank of Australia, Export and Finance Insurance Corporation, Classification Review Board, Office of Film and Literature Classification, and Austrade. To date, the ALRC has not received any submissions from these agencies. The NHMRC made a submission to this Inquiry but did not comment on whether its exemption should remain: National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

FOI Act. Some overseas jurisdictions, such as the United Kingdom and Hong Kong, exempt very few specified agencies from their privacy legislation.[88] It is, therefore, difficult to compare the exempt agencies that are listed in the FOI Act to overseas agencies that perform similar functions.

33.61 In the circumstances, there are two main options for reform. One is to remove the exemption on the basis that there does not appear to be sufficient justification for it. The other option is to require the relevant agencies to demonstrate to the Attorney-General that they warrant exemption from compliance with the *Privacy Act*, and if they fail to do so within 12 months, remove the exemption. The ALRC considers that the latter option is preferable, as it would give the relevant agencies a final opportunity to consider their position and make their case if they believe an exemption is warranted.

33.62 The ALRC considers that the current partial exemption that applies to AUSTRAC should remain. The exemption is a limited one and does not apply to AUSTRAC's administrative activities. The application of the proposed Unified Privacy Principles (UPPs) to AUSTRAC's existing exempt activities may cause difficulties for its operation, including the proposed principles concerning 'Collection', 'Specific Notification', 'Anonymity and Pseudonymity' and 'Identifiers'. In addition, the handling of information by AUSTRAC is governed by PSM 2005 and ACSI 33, as well as a secrecy provision that prohibits AUSTRAC officials from disclosing information collected, compiled or analysed by AUSTRAC. Unlike the other agencies listed in Schedule 2 of the FOI Act, the functions of AUSTRAC are more akin to those of law enforcement agencies. For these reasons, no strong case has been made out to remove the exemption.

33.63 In the ALRC's view, the current exemption from the FOI Act that applies to AUSTRAC should also remain. Individuals should not be alerted to the fact that a suspicious transaction report has been made about them. If the exemption from the FOI Act were removed, there is a potential for staff members of cash dealers and reporting entities to be at risk of retribution. In addition, in Chapter 15, the ALRC proposes that the proposed UPPs should apply to information privacy except to the extent that more specific primary or subordinate legislation covers a particular aspect of privacy or handling of personal information.[89] The removal of the exemption of AUSTRAC from the FOI Act would be inconsistent with that approach and undermine the objects of the AML/CTL Act and the *Financial Transaction Reports Act*.

33.64 In the ALRC's view, the ABC and SBS should not be exempt from the *Privacy Act* by virtue of their exempt status under the FOI Act. There are insufficient policy justifications for treating national broadcasters differently under the *Privacy Act* from media organisations in the private sector. Setting aside the question of access and

---

88 There are only four exemptions in the *Data Protection Act 1998* (UK) and three in *Personal Data (Privacy) Ordinance* (Hong Kong): see *Data Protection Act 1998* (UK) ss 30(2), 30(3), 31, 36; *Personal Data (Privacy) Ordinance* (Hong Kong) ss 52, 57, 61; and Ch 30.

89 See Proposal 15–3.

correction to their records, which is generally dealt with under the FOI Act, there is no justification for exempting the ABC and SBS from the privacy principles in relation to their program materials and datacasting content. The removal of the exemption would not affect their exempt status in relation to their acts and practices carried out in the course of journalism.

33.65 Currently, the ABC, SBS and other agencies discussed above are either partially or completely exempt from the operation of the FOI Act.[90] In Chapter 12, the ALRC proposes that an individual's right to access or correct his or her own personal information be dealt with in a new Part of the *Privacy Act*, and not under the FOI Act.[91] The ALRC invites submissions on what exceptions should apply to the proposed new provisions granting an individual the right to access his or her own personal information.[92] As part of that consideration, the ALRC is interested in views on whether these agencies should continue to be exempt from the general provision in the FOI Act granting an individual the right to access his or her own personal information.

Proposal 33–2 The following agencies listed in Schedule 2 Part I Division 1 and Part II Division 1 of the *Freedom of Information Act 1982* (Cth) should be required to demonstrate to the Attorney-General of Australia that they warrant exemption from the operation of the *Privacy Act*:

(a) Aboriginal Land Councils and Land Trusts;

(b) Auditor-General;

(c) National Workplace Relations Consultative Council;

(d) Department of the Treasury;

(e) Reserve Bank of Australia;

(f) Export and Finance Insurance Corporation;

(g) Australian Communications and Media Authority;

(h) Classification Board;

(i) Classification Review Board;

90 *Freedom of Information Act 1982* (Cth) s 7.
91 See Proposals 12–6, 12–7.
92 See Question 12–1.

(j) Australian Trade Commission; and

(k) National Health and Medical Research Council.

The Australian Government should remove the exemption from the operation of the *Privacy Act* for any of these agencies that, within 12 months, do not make an adequate case for retaining their exempt status.

Proposal 33–3 The *Privacy Act* should be amended to remove the exemption of the Australian Broadcasting Corporation and the Special Broadcasting Service listed in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth).

34. Other Public Sector Exemptions

Contents

Introduction 976
Royal commissions 976
Background 976
Submissions and consultations 977
ALRC's view 977
Australian Crime Commission 978
Background 978
Information management guidelines 980
Accountability and oversight mechanisms 980
International instruments 983
Overseas jurisdictions 984
Submissions and consultations 985
Options for reform 986
ALRC's view 986
Integrity Commissioner 987
Background 987
Oversight mechanisms 988
Submissions and consultations 989
ALRC's view 990
Other agencies with law enforcement functions 991
Background 991
Submissions and consultations 993
ALRC's view 994
Parliamentary departments 994
Background 994
Submissions and consultations 995
ALRC's view 996
State and territory authorities and prescribed instrumentalities 996
State and territory authorities 996
Prescribed state and territory instrumentalities 997
Should state and territory authorities be exempt from the *Privacy Act*? 998
State and territory government business enterprises 999
Opt-in provision 1002
Options for reform 1003
ALRC's view 1004

Introduction

34.1 The preceding chapters examine exemptions from the *Privacy Act 1988* (Cth) that apply to a number of agencies, including: defence and intelligence agencies; federal courts; and certain agencies listed in the *Freedom of Information Act 1982* (Cth). This chapter discusses the remaining public sector exemptions, including the exemption that applies to royal commissions, the Australian Crime Commission, the Integrity Commissioner, parliamentary departments, state and territory authorities and prescribed state and territory instrumentalities. In addition, the chapter considers whether law enforcement activities should be provided for under the *Privacy Act* by way of an exemption rather than exceptions.[1]

Royal commissions

Background

34.2 Commonwealth royal commissions are government inquiries established by the Governor-General of Australia pursuant to the *Royal Commissions Act 1902* (Cth)

> to make inquiry into and report upon any matter specified in the Letters Patent, and which relates to or is connected with the peace, order and good government of the Commonwealth, or any public purpose or any power of the Commonwealth.[2]

34.3 While royal commissions fall within the definition of an 'agency', their acts and practices are excluded from the definition of 'act or practice' and therefore from the operation of the *Privacy Act*.[3]

34.4 Commonwealth royal commissions have extensive coercive powers, including the power to summon witnesses and take evidence, authorise the application for search warrants, issue warrants for the arrest of witnesses who fail to appear, and inspect and retain any document or thing.[4] To support the use of these powers, the *Royal Commissions Act* creates a number of statutory offences for certain types of conduct, including where a person: fails to attend or produce documents; refuses to be sworn or give evidence; gives false or misleading evidence; bribes, deceives or injures a witness; or conceals, mutilates or destroys any document or thing that is likely to be required in evidence before a royal commission.[5]

34.5 Although Commonwealth royal commissions have powers that are usually exercised by courts and often follow procedures similar to those followed by courts, they cannot exercise judicial power.[6]

---

1 This distinction between an 'exception' and an 'exemption' is discussed below.
2 *Royal Commissions Act 1902* (Cth) s 1A.
3 *Privacy Act 1988* (Cth) s 7(1)(a)(v).
4 *Royal Commissions Act 1902* (Cth) ss 2, 4, 6B, 6F, 6FA.
5 Ibid ss 3, 6, 6AB, 6H–6K, 6M. See also ss 6L, 6N, 6O.
6 Only federal courts created by the Australian Parliament may exercise the judicial power of the Commonwealth: *Huddart, Parker & Co Pty Ltd v Moorehead* (1909) 8 CLR 330, 355.

> The duties of the commission are to inquire and report. It has, in order that it may effectively perform the duty of inquiry, certain powers which normally belong to judicial tribunals. But the function which is primarily distinctive of judicial power—the power to decide or determine—is absent. The commission can neither decide nor determine anything and nothing that it does can in any way affect the legal position of any person. Its powers and functions are not judicial.[7]

34.6 Royal commissions have general powers to order that any evidence be taken in private. They may also prohibit the publication of any evidence, contents of any document, or a description of any thing, produced before, or delivered to, the commission, or any information that might enable a person who has given evidence before the commission to be identified.[8]

34.7 Privacy concerns have been raised where inquiries by royal commissions are held in public. One commentator argues that royal commissions have greater powers than courts to force revelations and even confessions, because they do not presume either innocence or guilt. It was argued, therefore, that there is a risk that individuals who are being investigated may be forced to make embarrassing revelations and face exposure, humiliation and adverse publicity without regard for the appropriate balance between privacy and open justice.[9]

34.8 In New Zealand, royal commissions and other commissions of inquiries are completely exempt from the *Privacy Act 1993* (NZ).[10]

Submissions and consultations

34.9 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether royal commissions should be exempt from the operation of the *Privacy Act*.[11] The ALRC has received few submissions in response to this question. The Office of the Privacy Commissioner (OPC) submitted that, although the *Privacy Act* may not be the appropriate instrument to deal with concerns regarding the operations of royal commissions, 'attention should be given to developing information handling standards for royal commissions that promote respect for privacy'. The OPC also suggested that the matter be referred to the Attorney-General.[12]

ALRC's view

34.10 Royal commissions serve the important function of inquiring into matters of public interest. Central to the performance of that function is the ability of royal commissions to obtain information that may be unavailable by other means of

---

7 *Lockwood v Commonwealth* (1954) 90 CLR 177, 181.
8 *Royal Commissions Act 1902* (Cth) s 6D(3)–(5).
9 M Rayner, 'Commissions and Omissions' (1996) 6(10) *Eureka Street* 14.
10 *Privacy Act 1993* (NZ) s 2(1) (definition of 'agency').
11 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
12 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

investigation or inquiry. Although they do not exercise judicial power, they are given powers that are usually exercised by courts.

34.11 In the ALRC's view, the exemption of royal commissions from the *Privacy Act* is warranted. The ALRC agrees with the OPC, however, that information-handling guidelines that apply to royal commissions should be developed. The Attorney-General's Department, in consultation with the OPC, should develop such guidelines.

Proposal 34–1 The Attorney-General's Department, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for royal commissions to assist in ensuring that the personal information they handle is protected adequately.

Australian Crime Commission

Background

34.12 The Australian Crime Commission (ACC) was established under the *Australian Crime Commission Act 2002* (Cth) (ACC Act) to counter serious and organised crime. The ACC was formed by replacing the National Crime Authority (NCA), and absorbing the functions of the Australian Bureau of Criminal Intelligence (ABCI)[13] and the Office of Strategic Crime Assessments.[14] The functions of the ACC include: collecting and analysing criminal intelligence; setting national criminal intelligence priorities; providing and maintaining criminal intelligence systems; and investigating federally relevant criminal activity and undertaking taskforces.[15]

34.13 Although the ACC falls within the definition of 'agency' under the *Privacy Act*, the acts and practices of the ACC are excluded from the definition of 'an act or practice'.[16] In addition, s 7(2) of the Act exempts the ACC from compliance with the tax file number provisions of the Act. The ACC therefore is completely exempt from the operation of the Act.

---

13 The ABCI was established to facilitate the exchange of criminal intelligence among federal, state and territory law enforcement agencies, anti-corruption bodies and regulatory agencies. It was responsible for the analysis and dissemination of criminal intelligence, but relied on these agencies for the collection of information: Australian Crime Commission, *Annual Report 2002–2003* (2003), 152; Parliament of Australia—Parliamentary Joint Committee on the Australian Crime Commission, *The Law Enforcement Implications of New Technology* (2001).

14 The Office of Strategic Crime Assessments was an element of the Australian Government Attorney-General's Department preparing national level strategic law enforcement intelligence: Australian Crime Commission, *Submission to the Inquiry by the Parliamentary Joint Committee of Public Accounts and Audit Management and Integrity of Electronic Information in the Commonwealth*, 1 January 2003, 4.

15 Australian Crime Commission, *Australian Crime Commission Profile—Dismantling Serious and Organised Criminal Activity* (2007) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 15 August 2007, 1.

16 *Privacy Act 1988* (Cth) s 7(1)(a)(iv).

34.14 Acts and practices in relation to records that have originated with, or have been received from, the ACC or the Board of the ACC (ACC Board) are also exempt.[17] Accordingly, agencies and organisations receiving a record from the ACC are exempt from the operation of the *Privacy Act* in relation to that record. Furthermore, since the ACC falls within the definition of an 'enforcement body' under the Act,[18] personal information may be disclosed by an organisation to the ACC in certain circumstances, including where the disclosure is for the purpose of preventing, detecting, investigating or prosecuting criminal offences, or prevention, detection, investigation or remedying of seriously improper conduct.[19]

34.15 The ACC has a range of special powers that are used 'where ordinary law enforcement methodologies are ineffective'.[20] These special powers include the power to conduct examinations, issue a summons requiring a person to attend an examination to give evidence under oath or affirmation, and require the production of any document or thing.[21] Failure to attend an examination, or to answer questions or produce specified documents or things at an examination, is an offence that is punishable by fines and imprisonment.[22]

34.16 The ACC Act contains a secrecy provision that prohibits ACC officials and staff from recording, communicating or divulging any information acquired by reason of, or in the course of, the performance of their duties under the Act.[23]

34.17 There is a tension between privacy and law enforcement, particularly in the context of organised crime.

> By definition, effective law enforcement and investigation of organised crime requires maximum disclosure of information by government departments to law enforcement agencies. In theory, a maximum flow of information between law enforcement agencies is also required. At the same time, governments have an interest in preventing the unjustified or unnecessary disclosure of information and protecting citizens from unjustified invasions of their privacy by state officials.[24]

---

17 Ibid s 7(1)(h).
18 Ibid s 6(1).
19 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 203.
20 Australian Crime Commission, *Australian Crime Commission Profile—Dismantling Serious and Organised Criminal Activity* (2007) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 15 August 2007, 1.
21 *Australian Crime Commission Act 2002* (Cth) pt II div 2.
22 Ibid s 30.
23 Ibid s 51. The section applies to the CEO of the ACC, members of the ACC Board, members of the ACC staff and examiners. *Australian Crime Commission Act 2002* (Cth) ss 24A, 46B.
24 C Corns, 'Inter Agency Relations: Some Hidden Obstacles to Combating Organised Crime?' (1992) 25 *Australia and New Zealand Journal of Criminology* 169, 177.

Information management guidelines

34.18 The primary documents that prescribe the requirements for the management and security of information by the ACC include the *Protective Security Manual* (PSM 2005), the *Australian Government Information Technology Security Manual* (ACSI 33) and the *ACC Policy and Procedures Manual*.[25] The *ACC Policy and Procedures Manual* is a classified document.[26]

34.19 PSM 2005 is a policy document that sets out guidelines and minimum standards in relation to protective security for agencies and officers. It also applies to contractors and their employees who perform services for the Australian Government. In particular, Part C of the PSM 2005 provides 'guidance on the classification system and the protective standards required to protect both electronic- and paper-based security classified information'.[27] The part sets out minimum standards addressing the use, access, copying, storage, security and disposal of classified information.

34.20 Agencies are also required by the PSM 2005 to comply with the ACSI 33. ACSI 33 has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to agencies on the protection of their electronic information systems.[28]

Accountability and oversight mechanisms

34.21 The ACC is subject to oversight through a number of mechanisms described below.

Ministerial oversight

34.22 The ACC is responsible to the Minister for Justice and Customs. The Chair of the ACC Board must keep the Minister informed of the general conduct of the ACC in the performance of the ACC's functions. He or she must comply with the Minister's request for information concerning any specific matter relating to the ACC's conduct

---

25 Australian Crime Commission, *Submission to the Inquiry by the Parliamentary Joint Committee of Public Accounts and Audit Management and Integrity of Electronic Information in the Commonwealth*, 1 January 2003, 11. The ACC is also required to comply with *Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification* (ACSI 37) published by the DSD. ASCI 37 is a controlled document that outlines certain requirements for physical security.

26 In addition, there is a range of state legislative and guidance documents prescribing the ACC's requirements for the management and security of information entrusted to the ACC: Ibid, 11.

27 Australian Government Attorney-General's Department, *Protective Security Manual (PSM 2005)* <www.ag.gov.au/www/agd/agd.nsf/Page/National_security> at 31 July 2007.

28 Defence Signals Directorate, *Australian Government Information Technology Security Manual (ACSI 33)* (2004). There are two versions of ACSI 33. The security-in-confidence version contains the security policies and guidance for all classifications. The unclassified version only contains policies and guidance for the following classifications: public domain, unclassified, in-confidence, restricted, and protected. An unclassified version of ACSI 33 is available on the DSD's website: Defence Signals Directorate, *ACSI 33—Australian Government Information and Communications Technology Security Manual* <www.dsd.gov.au/library/infosec/acsi33.html> at 8 August 2007.

in the performance of its functions.[29] The Minister may give directions or issue guidelines to the ACC Board in relation to the performance of the Board's functions.[30]

ACC Board

34.23 The ACC Board consists of the Commissioner of the Australian Federal Police (AFP), the Secretary of the Attorney-General's Department, the Chief Executive Officer (CEO) of the Australian Customs Service, the Chairperson of the Australian Securities and Investments Commission (ASIC), the Director-General of Security, eight state and territory police commissioners, and the CEO of the ACC (as a non-voting member).[31]

34.24 The Board's functions include: determining national criminal intelligence priorities; authorising the ACC to undertake intelligence operations or to investigate matters relating to federally relevant criminal activity; determining whether an operation or investigation is a special operation or investigation;[32] determining the classes of persons to participate in an intelligence operation or investigation; establishing task forces; disseminating strategic criminal intelligence assessments to law enforcement agencies, foreign law enforcement agencies, or prescribed federal, state or territory agencies. It is also required to report to the Inter-Governmental Committee on the ACC's performance.[33]

Inter-Governmental Committee

34.25 The Inter-Governmental Committee on the ACC (IGC) consists of the Minister for Justice and Customs, and federal, state and territory police or justice ministers.[34] It was established under the ACC Act to monitor the work of the ACC and the ACC Board, oversee the strategic direction of the ACC and the ACC Board, and receive reports from the Board for transmission to federal, state and territory governments.[35] Where the ACC Board has determined that an investigation or operation is a special investigation or operation, the IGC may request that the Chair of the ACC Board

---

29 *Australian Crime Commission Act 2002* (Cth) s 59.

30 Ibid s 18.

31 Ibid ss 7B, 7G(3).

32 The ACC Board may determine that an intelligence operation is a special operation if it considers that methods of collecting the criminal information and intelligence that do not involve the use of powers in the ACC Act have not been effective: Ibid s 7C(2). The Board may determine that an investigation into matters relating to federally relevant criminal activity is a special investigation if it considers that ordinary police methods of investigation into the matters are unlikely to be effective: s 7C(3). The making of such a determination by the ACC Board allows an eligible person within the ACC to apply for search warrants; or an ACC examiner to apply to the Federal Court for the surrender of a passport, conduct examinations, summon a person to attend an examination, require a person produce documents or other things, or apply to the Federal Court for a warrant where a witness fails to surrender a passport: ss 22–25A, 28, 29, 31.

33 Ibid s 7C(1).

34 Ibid s 8(1).

35 Ibid s 9(1).

provide the IGC with further information in relation to the determination.[36] The IGC also has the power to revoke that determination.[37]

Parliamentary Joint Committee

34.26 The Parliamentary Joint Committee on the ACC comprises members from both the Senate and the House of Representatives.[38] It is responsible for monitoring and reviewing the performance by ACC, reporting to the Parliament in relation to the ACC, examining the ACC's annual reports, examining trends and changes in criminal activities, practices and methods, and recommending changes to the functions, structure, powers and procedures of the ACC to the Parliament, and conducting inquiries.[39]

Commonwealth Ombudsman

34.27 Under the *Ombudsman Act 1976* (Cth),[40] the Commonwealth Ombudsman has power to investigate complaints about the ACC. It also has oversight over the ACC's use of:

- controlled operations under Part IAB of the *Crimes Act 1914* (Cth);
- surveillance devices under the *Surveillance Devices Act 2004* (Cth); and
- telephone intercept warrants under the *Telecommunications (Interception) Act 1979* (Cth).[41]

34.28 The Commonwealth Ombudsman received nine complaints about the ACC in 2005–06 and 12 in 2004–05. It commented that while it was not obliged to make inquires of the ACC upon receipt of a complaint, the ACC was highly responsive to its inquires. In its annual report for 2005–06, the Commonwealth Ombudsman stated that:

> While the ACC is not required to proactively report complaints to the Ombudsman's office, we continue to have an open working relationship with the ACC. The ACC

---

36 Ibid s 9(2). The Chair of the ACC Board only may refuse to give that information if it considers that the disclosure of the information to the public could prejudice the safety or reputation of persons or the operation of the law enforcement agencies. If the information is withheld on this ground, the IGC may refer its request to the minister for his or her determination: *Australian Crime Commission Act 2002* (Cth) s 9(3), (6).

37 *Australian Crime Commission Act 2002* (Cth) s 9(7).

38 Ibid s 53.

39 Ibid s 55.

40 *Ombudsman Act 1976* (Cth).

41 *Crimes Act 1914* (Cth) pt IAB div 2A; *Surveillance Devices Act 2004* (Cth) s 55(2); *Telecommunications (Interception) Act 1979* (Cth) s 82. A 'controlled operation' is an operation that: involves the participation of law enforcement officers; is carried out for the purpose of obtaining evidence in relation to a serious Commonwealth offence or a serious state offence that has a federal aspect; and may involve a law enforcement officer or other person in acts or omissions that would constitute an office: *Crimes Act 1914* (Cth) s 15H.

> notifies the Ombudsman's office about significant matters, allowing us to consider whether further investigation by Ombudsman staff is warranted.[42]

34.29 The Commonwealth Ombudsman stated that it has inspected the records of the ACC on six occasions, and was generally satisfied with the level of compliance by the ACC. It also reported that all of its recommendations following finalisation of inspections in 2005–06 were accepted by the ACC.[43]

Australian Commission for Law Enforcement Integrity

34.30 The Integrity Commissioner, supported by the Australian Commission for Law Enforcement Integrity (ACLEI), is responsible for preventing, detecting and investigating serious corruption issues in agencies with law enforcement functions, including the ACC.[44] The functions of the Integrity Commissioner include, among other things, investigating and reporting on corruption issues, conducting public inquiries into corruption, and handling information and intelligence relating to corruption.[45]

Auditor-General

34.31 The Auditor-General is an independent officer of the Australian Parliament responsible for performing financial and performance audits of certain agencies, including the ACC.[46] The Auditor-General has broad information-gathering powers and authority to have access to Commonwealth premises.[47]

International instruments

34.32 International privacy instruments commonly provide for exceptions to the principles that apply to criminal investigations. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines) recognise that member countries may apply the OECD Guidelines differently to different kinds of personal data or in different contexts, such as criminal investigations.[48] The OECD Guidelines also state that criminal investigative activities are one area where, for practical or policy reasons, an individual's knowledge or consent cannot be considered necessary for the collection of his or her personal data.[49]

---

42 Commonwealth Ombudsman, *Annual Report 2005–2006* (2006), 91.

43 Ibid, 26, 92.

44 *Law Enforcement Integrity Commissioner Act 2006* (Cth) ss 5(1) (definition of 'law enforcement agency'), 7, 15. At present, the Act only applies to the ACC, AFP and the former NCA.

45 Ibid s 15.

46 *Auditor-General Act 1997* (Cth) ss 11, 15, 18; *Financial Management and Accountability Act 1997* (Cth) s 5; *Financial Management and Accountability Regulations 1997* (Cth) sch 1 pt 1 item 108A.

47 *Auditor-General Act 1997* (Cth) pt 5 div 1.

48 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Memorandum, [47].

49 Ibid, Memorandum, [47].

34.33 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains exceptions to the privacy principles, including the processing of data necessary for the prevention, investigation, detection and prosecution of criminal offences,[50] and concerning public security, state security and the activities of the state in areas of criminal law.[51] Article 13 of the EU Directive provides that member states may provide for exceptions from specified data processing principles if they are necessary to safeguard public security and the prevention, investigation, detection and prosecution of criminal offences. The principles from which such exceptions are permitted include those relating to: data quality; information to be given to the individual concerned; an individual's right of access to data; and the publicising of processing operations.[52]

34.34 Like the EU Directive, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework states that it is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests.[53]

Overseas jurisdictions

34.35 Criminal investigation is also a common exception to data protection principles in overseas jurisdictions, such as, the United Kingdom, New Zealand and Hong Kong. Under the *Data Protection Act 1998* (UK), certain data protection principles do not apply if the application of those principles would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature. The principles that do not apply include: purpose of collection; fair processing by notification to the individual concerned; an individual's rights of access and correction; data quality; data retention; and an individual's right to prevent processing.[54]

34.36 The New Zealand *Privacy Act 1993* provides for exceptions to some of the information privacy principles where non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences, and the enforcement of a law imposing a pecuniary penalty.[55] The relevant principles include those concerning: collection of personal data directly from the individual concerned;

---

50 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 13(1)(d).

51 Ibid, art 3(2).

52 Ibid, art 13. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recital 16 and 43.

53 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13]. See also Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [31].

54 *Data Protection Act 1998* (UK) s 29.

55 *Privacy Act 1993* (NZ) ss 6 (Principles 2, 3, 10, 11), 27.

notification to individuals about certain matters; and use and disclosure of personal information.

34.37 Hong Kong privacy legislation also provides for exceptions to the use and access principles where compliance with those principles is likely to prejudice the prevention or detection of crime, the apprehension, prosecution or detention of offenders, and other unlawful conduct.[56]

Submissions and consultations

34.38 In IP 31, the ALRC asked whether the ACC should be exempt from the *Privacy Act*, and, if so, what is the policy justification for the exemption.[57] Few stakeholders responded to this question.

34.39 The OPC noted that the exemption that applies to the ACC originally applied to the NCA.[58] The reasons behind the exemption that applied originally

> appear to have been based on the NCA's coercive powers, unique to Commonwealth law enforcement, which allowed the collection of personal information of a speculative and untested nature.[59]

34.40 The OPC submitted that, since the absorption of the ABCI's functions into the ACC, much of the information collected by the former ABCI is now collected and stored on the ACC's intelligence databases. In addition, the OPC observed that many of the records held in these databases are sourced from the AFP, the Australian Transaction Analysis Centre (AUSTRAC), ASIC and other agencies that are covered by the *Privacy Act*.[60]

34.41 The OPC also stated that some agencies that perform a law enforcement function—for example, the AFP, AUSTRAC, ASIC and the Australian Taxation Office—are covered by the *Privacy Act*, and that it has issued guidance on how the *Privacy Act* provides for law enforcement needs.[61] The OPC submitted that 'in view of the changed role of the ACC over the years … it may be timely to reassess the suitability of the current ACC exemption from the *Privacy Act*'. The OPC suggested that 'one option [for reform] could be for the administrative operations of the ACC to be covered by the *Privacy Act*'.[62]

---

56 *Personal Data (Privacy) Ordinance* (Hong Kong) s 58.
57 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.
58 See Explanatory Memorandum, Privacy Bill 1988 (Cth) [46].
59 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 28.
60 Ibid, 28.
61 Ibid, 28.
62 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

34.42 It was suggested in another submission that the ACC should be partially exempt from the *Privacy Act*, but only on a case-by-case basis and where there is sufficient oversight.[63]

Options for reform

34.43 There are essentially three options for reform. One option is to remove the exemption that applies to the ACC but amend the definition of 'law enforcement body' to include the ACC. This would ensure that the ACC is subject to the privacy principles except to the extent that non-compliance is required for the performance of its law enforcement activities. It is also consistent with the approach under international instruments and some overseas privacy legislation.

34.44 Another option is to modify the exemption so that the ACC is covered by the *Privacy Act* in respect of its administrative operations, such as the handling of its employee records.

34.45 A third option is to require the ACC to comply with information-handling guidelines, to be developed in consultation with the OPC and issued by the Minster for Justice and Customs. This approach is similar to the approach taken in relation to exempt defence and intelligence agencies, which are required to comply with ministerial directions or guidelines in relation to privacy.[64]

ALRC's view

34.46 As the discussion in Chapter 1 illustrates, privacy is not an absolute right. Privacy interests must be balanced with other competing public interests, including 'the need of society to create and enforce rules of personal and corporate behaviour for the common good'.[65] In a recent review of the ACC Act, the Parliamentary Joint Committee on the ACC commented that:

> Given the particularly violent and pernicious nature of organised crime, history has shown the need to create specialist crime fighting bodies with significant powers to combat these organised crime networks. However, it is evident from the description of the ACC's powers … that the actions of the ACC have the potential to impact profoundly on the individual citizen's freedom and privacy.[66]

34.47 Since the ACC is already subject to information management guidelines and a significant amount of oversight, there may be an argument for its exemption from the *Privacy Act*. There are, however, two major arguments that support imposing privacy requirements on the ACC through the *Privacy Act*—first, there is a significant potential for the ACC's activities to impact on the privacy of individuals; and secondly, other federal law enforcement agencies are covered by the Act. Currently, there are a number

---

63 K Handscombe, *Submission PR 89*, 15 January 2007.

64 See discussion in Ch 31.

65 Parliament of Australia—Parliamentary Joint Committee on the Australian Crime Commission, *Review of the Australian Crime Commission Act 2002* (2005), [5.85].

66 Ibid, [5.86].

of specific exceptions to the IPPs that allow federal law enforcement agencies to carry out their law enforcement functions. There are also a number of specific exceptions to the proposed Unified Privacy Principles (UPPs) that would allow federal law enforcement agencies to function effectively.

34.48 As the OPC noted in its submission, many of the records held in the ACC's databases are collected from the AFP, AUSTRAC, ASIC and other agencies that are covered by the *Privacy Act*.[67] In addition, other agencies that perform a law enforcement function are covered by the *Privacy Act*. The ALRC's preliminary view is, therefore, that the ACC should not be exempt from the operation of the *Privacy Act*. Whether privacy principles should provide for law enforcement activities undertaken by law enforcement agencies, such as the ACC, by way of an exemption rather than an exception, is discussed below.

Proposal 34–2 The *Privacy Act* should be amended to remove the exemption that applies to the Australian Crime Commission and the Board of the Australian Crime Commission by repealing s 7(1)(a)(iv), (h) and 7(2) of the Act.

Integrity Commissioner

Background

34.49 Commencing operation in December 2006, the ACLEI was established to detect and investigate corruption in the AFP, the ACC, the former NCA and prescribed Australian Government agencies with law enforcement functions.[68] It is headed by the Integrity Commissioner, whose functions include: investigating and reporting on corruption issues; referring corruption issues to law enforcement agencies for investigation; managing, overseeing or reviewing the investigation of corruption by law enforcement agencies; conducting public inquiries into corruption; collecting, analysing and communicating information and intelligence relating to corruption; and making reports and recommendations to the responsible minister concerning the need or desirability of legislative or administrative actions on corruption issues.[69]

34.50 The Integrity Commissioner has similar powers to a royal commission, including the power to execute search warrants, conduct public or private hearings,

---

67 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994), 28.

68 *Law Enforcement Integrity Commissioner Act 2006* (Cth) ss 5(1) (definition of 'law enforcement agency'), 7, 15. No additional Australian Government agencies have yet been prescribed as law enforcement agencies under the Act.

69 Ibid s 15.

summon people to attend hearings to give evidence or produce any document or thing, and take possession of, copy or retain any document or thing.[70]

34.51 The Integrity Commissioner is exempt from the operation of the *Privacy Act*.[71] Acts and practices in relation to a record that has originated with, or has been received from, the Integrity Commissioner or a staff member of the ACLEI, are also exempt.[72] In addition, since the Integrity Commissioner is an 'enforcement body' under the Act,[73] personal information may be disclosed by an organisation to the Integrity Commissioner in certain circumstances, including where the disclosure is for the purpose of preventing, detecting, investigating or prosecuting criminal offences, or the prevention, detection, investigation or remedying of seriously improper conduct.[74]

34.52 The *Law Enforcement Integrity Commissioner Act 2006* (Cth) imposes certain confidentiality requirements on ACLEI staff.[75] A current or former ACLEI staff member must not record, divulge or communicate any information acquired in the course of carrying out his or her duties, except in the performance of those duties.[76]

Oversight mechanisms

34.53 The Integrity Commissioner is required to give an annual report to the Minister for Justice and Customs to be presented to the Parliament.[77] The Commissioner is also required to give investigation and inquiry reports to the Minister if public hearings were held in the course of an investigation.[78] The Minister must remove certain information—such as information that may endanger a person's life or physical safety or prejudice certain proceedings—before tabling such a report in Parliament.[79] The Integrity Commissioner may also give special reports to the Minister on the operations of his office for presentation to the Parliament.[80]

34.54 The Integrity Commissioner must notify the Minister of any issue concerning the corrupt conduct of a current or former ACLEI staff member, and staff are under a similar obligation to report corruption by the Integrity Commissioner.[81] Any member of the public also may refer to the Minister an allegation or information raising an issue concerning corruption in the ACLEI.[82] The Minister may refer the issue to the Integrity Commissioner for investigation, or authorise a special investigator—who has the same

70 Ibid pt 9.
71 *Privacy Act 1988* (Cth) s 7(1)(a)(iiia).
72 Ibid s 7(1)(ga).
73 Ibid s 6(1).
74 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 203.
75 Ibid pt 13 div 5
76 Ibid s 207.
77 Ibid s 201.
78 Ibid s 203(1).
79 Ibid s 203(2).
80 Ibid s 204.
81 Ibid s 153.
82 Ibid s 154.

investigative and reporting powers that would be available to ACLEI—to investigate the issue.[83]

34.55 After the first three years of operation, the Minister must cause an independent review of the ACLEI Act to be undertaken, unless a parliamentary committee or the Parliament Joint Committee on the ACLEI has started or completed a review of the operation of the Act before the end of the three year period.[84]

34.56 The *Law Enforcement Integrity Commissioner Act* established a Parliamentary Joint Committee on the ACLEI.[85] The functions of the Committee are to monitor and review the Integrity Commissioner's performance of his or her functions, examine the annual reports and special reports of the Integrity Commissioner, examine and report on trends and changes in corruption issues and recommend changes to the functions, powers and procedures of the Integrity Commissioner, and conduct an inquiry into any question in connection with the Committee's duties that is referred by either House of Parliament.[86]

34.57 In addition, the Integrity Commissioner is subject to regular inspection and monitoring by the Commonwealth Ombudsman in relation to the exercise of his or her powers to:

- carry out controlled operations under Part 1AB of the *Crimes Act*;
- use surveillance devices under the *Surveillance Devices Act*; and
- undertake telecommunications interception and access stored communications under the *Telecommunications (Interception) Act*.[87]

Submissions and consultations

34.58 In IP 31, the ALRC asked whether the Integrity Commissioner should be exempt from the *Privacy Act*.[88] The ALRC has received few submissions in response to this question. The OPC submitted that it would be desirable if the ACLEI

> developed information handling guidelines to assist in ensuring that the personal information it handles is adequately protected.

83 Ibid s 154.
84 Ibid s 223A.
85 Ibid pt 12 div 4.
86 Ibid s 215.
87 *Telecommunications (Interception) Act 1979* (Cth) s 5(3B). See also Commonwealth Ombudsman, *Annual Report 2005–2006* (2006), 92.
88 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.

> The Integrity Commissioner (Acting) has indicated that he would be amenable for his Office to develop such guidelines with assistance as necessary from the Office of the Privacy Commissioner.
>
> As with the ACC, another option could be for the administrative operations of the ACLEI to be covered by the *Privacy Act*.[89]

ALRC's view

34.59 There is an important public interest in ensuring that government agencies that are vested with coercive powers are monitored and held accountable. The creation of government agencies that perform an oversight role, such as the Integrity Commissioner, serves that public interest. This public interest should, however, be balanced with the need to protect the privacy of personal information about individuals.

34.60 In the ALRC's view, such a balance could be achieved by partially exempting the Integrity Commissioner from the operation of the *Privacy Act* in respect of his or her investigative and inquiry functions. There is, however, no sound policy reason why the Integrity Commissioner should be exempt in respect of the administrative operations of his or her office, such as the handling of employee records. In addition, the Integrity Commissioner should be subject to information-handling guidelines in respect of the non-administrative operations of his or her office.

34.61 This is consistent with the ALRC's proposals in relation to the Inspector-General of Intelligence and Security (IGIS), who oversees the operation of the defence and intelligence agencies. In Chapter 31, the ALRC proposes that the IGIS be covered by the *Privacy Act* in respect of the administrative operations of his or her office. In addition, the ALRC proposes that the IGIS, in consultation with the OPC, develop and publish information-handling guidelines to ensure that the privacy of personal information handled by the Integrity Commissioner in respect of his or her office's non-administrative operations is protected adequately.[90]

Proposal 34–3 The *Privacy Act* should be amended to apply to the Integrity Commissioner in respect of the administrative operations of his or her office.

Proposal 34–4 The Integrity Commissioner, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity is protected adequately.

89 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.
90 Proposals 31–6 and 31–7.

Other agencies with law enforcement functions

Background

34.62 With the exception of the ACC, law enforcement agencies and other agencies with law enforcement functions are covered by the *Privacy Act*. For example, the AFP is expressly included within the definition of 'agency' under the Act and therefore is required to comply with the IPPs.[91]

34.63 Given the need to balance the privacy of individuals with the public interest in law enforcement and the regulatory objectives of government, the *Privacy Act* provides for specific exceptions to the IPPs. Under IPPs 10 and 11, agencies are permitted to use or disclose personal information in certain circumstances. In the context of law enforcement, two exceptions are of particular relevance. IPPs 10.1(c) and 11.1(e) authorise the use or disclosure of personal information if it is 'reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'.[92] IPPs 10.1(c) and 11.1(d) also allow the use or disclosure of personal information by agencies if the use or disclosure is 'required or authorised by or under law'.[93]

34.64 In addition, some IPPs are interpreted to include law enforcement considerations within their terms. For example, IPP 2 provides that an agency collecting personal information about an individual is to 'take such steps (if any) as are, in the circumstances, reasonable' to ensure that the individual concerned is generally aware of the purpose for which the information is being collected and other matters. In the law enforcement context, 'reasonable steps' have been interpreted to mean taking no step at all in circumstances where a suspect should not be alerted to the fact of the collection of personal information about him or her.

34.65 Furthermore, under IPPs 5.2, 6 and 7, if an agency is required or authorised under an applicable Commonwealth law to do so, it may refuse to provide an individual with information about what personal information is held about him or her, access to a record or the right to correct or amend documents containing personal information about the individual held by the agency. Section 37 of the *Freedom of Information Act 1982* (Cth) (FOI Act) provides that an agency does not have to provide access to, or allow correction of, documents if the disclosure of the document would, or could reasonably be expected to:

---

91 *Privacy Act 1988* (Cth) sch 3, NPP 2, note 1.

92 Where personal information is used or disclosed for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the agency must include in the record containing that information a note of that use or disclosure: Ibid s 14, IPPs 10.2, 11.2.

93 See also Ch 13.

- prejudice the conduct of an investigation or the enforcement or proper administration of the law in a particular instance;
- disclose the existence or identity of a confidential source of information in relation to the enforcement or administration of the law;
- endanger the life or physical safety of any person;
- prejudice the fair trial or impartial adjudication of a particular case;
- disclose lawful methods for dealing with breaches or evasions of the law that would, or would be reasonably likely to, prejudice the effectiveness of those methods; or
- prejudice the maintenance or enforcement of lawful methods for the protection of public safety.

34.66 In addition to exceptions to the IPPs that apply to law enforcement agencies, the *Privacy Act* also contains exceptions to the NPPs that allow organisations to cooperate lawfully with agencies performing law enforcement functions, by allowing an organisation to use, disclose, or deny access to, personal information for certain law enforcement or regulatory purposes.[94]

34.67 NPP 2.1 provides that an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection except in specified circumstances. The specified circumstances include the use and disclosure of personal information where it is: for the purposes of reporting or investigating unlawful activity; required or authorised by or under law; and reasonably necessary for a range of activities carried out by, or on behalf of, an enforcement body.[95] The range of activities include:

> (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
>
> (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
>
> (iii) the protection of the public revenue;
>
> (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
>
> (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.[96]

---

94 *Privacy Act 1988* (Cth) s 6; sch 3, NPPs 2.1, 6.1.
95 Ibid sch 3, NPP 2.1(f)–(h).
96 Ibid sch 3, NPP 2.1(h).

34.68 NPP 6.1 provides further that an organisation must, on request by an individual, provide the individual with access to personal information it holds about the individual, subject to certain exceptions. These exceptions include where: providing access would be unlawful; denying access is required or authorised by or under law; providing access would be likely to prejudice an investigation of possible unlawful activity; providing access would be likely to prejudice certain law enforcement activities; and an enforcement body performing a lawful security function asks the organisation not to provide access to the information, on the basis that providing access would be likely to cause damage to the security of Australia.[97]

34.69 As discussed above, the OECD Guidelines, the EU Directive and some overseas legislation also provide for certain exceptions to their data protection principles for the purposes of criminal investigation. Other jurisdictions, however, provide for law enforcement activities in their privacy legislation by way of exemptions rather than exceptions. In New South Wales, for example, there are detailed exemptions for law enforcement bodies, such as the state and territory police force, the New South Wales Crime Commission, the AFP, the ACC, and the state and territory Directors of Public Prosecutions.[98] Similarly, in Victoria, a law enforcement agency is exempt from compliance with certain privacy principles under the *Information Privacy Act 2000* (Vic) in specified circumstances.[99]

Submissions and consultations

34.70 In IP 31, the ALRC asked whether there are any other agencies that should be exempt, either completely or partially, from the *Privacy Act*.[100] In response, the AFP submitted that the ALRC should consider 'how the protection of personal and sensitive information is best balanced with the broad and unpredictable nature of policing activities'. The AFP observed that, although law enforcement functions and requirements can be understood to be within the terms of the IPPs, there is no explicit recognition of operational policing in the privacy principles concerning collection (IPPs 1–3), and access and correction (IPPs 6 and 7). It suggested that an option for reform would be to extend the exceptions to the IPPs in line with the approach under the EU Directive, and the New South Wales and Victorian privacy legislation. The AFP submitted that this approach is a more transparent way for the *Privacy Act* to set out the range of circumstances in which police can collect, analyse, and disclose personal and sensitive information. It stated that this would also clarify the interaction between the *Privacy Act*, and the secrecy and disclosure provisions in other legislation.[101]

---

97 Ibid sch 3, NPP 6.1(g)–(k).

98 *Privacy and Personal Information Protection Act 1998* (NSW) s 3(1).

99 Examples of law enforcement agencies include the state or territory police force, the AFP and the ACC: *Information Privacy Act 2000* (Vic) s 3.

100 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–3.

101 Australian Federal Police, *Submission PR 186*, 9 February 2007.

ALRC's view

34.71 It is clear that requiring compliance with some of the privacy principles by law enforcement agencies would be inconsistent with the performance of their law enforcement functions in certain circumstances. For example, law enforcement agencies should generally not be required to alert a suspect to the collection of his or her personal information and should be able to disclose information for law enforcement purposes.

34.72 Currently, the *Privacy Act*, in conjunction with other Commonwealth legislation (such as the FOI Act), provides a number of exceptions to the privacy principles that allow such agencies to carry out their law enforcement activities. In its submission, the AFP suggested that these exceptions should be provided for by way of an exemption instead. In Chapter 30, a distinction is drawn between an *exemption* and an *exception*. An *exemption* applies where a specified entity or a class of entity is not required to comply with the privacy principles that would otherwise be applicable to it. An *exception* applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct.

34.73 One argument for providing for law enforcement activities by way of an exemption rather than an exception is that it would clarify which law enforcement agencies are not required to comply with privacy principles when carrying out their law enforcement functions. The ALRC , however, does not have sufficient information to make a proposal and would be interested in views from a larger number of stakeholders on whether the current exceptions to the privacy principles for law enforcement purposes should be amended and set out in the form of an exemption for agencies that perform law enforcement functions.

Question 34–1 Should the *Privacy Act* be amended to set out, in the form of an exemption, the range of circumstances in which agencies that perform law enforcement functions, such as the Australian Federal Police and the Australian Crime Commission, are not required to comply with specific privacy principles?

Parliamentary departments

Background

34.74 Section 81(1)(a) of the *Parliamentary Service Act 1999* (Cth) provides that, in any Act other than the *Privacy Act*, a reference to an 'agency' includes a reference to a Department of the Parliament established under the *Parliamentary Service Act*. Since Departments of the Parliament established under the *Parliamentary Service Act* fall outside the definition of an 'agency' under the *Privacy Act*, they are exempt from the operation of the *Privacy Act*. These departments include the Department of the Senate,

the Department of the House of Representatives and the Department of Parliamentary Services (DPS).[102] The Department of the Senate and the Department of the House of Representatives provide advice and support to the Senate and the House of Representatives respectively, and to committees, senators and members.[103]

34.75 The DPS is headed by the Parliamentary Service Commissioner, whose functions are to give advice to Presiding Officers of both Houses of Parliament on the management policies and practices of the Parliamentary Service,[104] and if requested by the Presiding Officers, inquire into and report on matters relating to the Parliamentary Service that are specified in the request. The DPS is responsible for providing information analysis and advice to the Australian Parliament, maintaining and facilitating access to the Parliamentary Library's electronic and print information resources and providing a range of other services, such as information technology, broadcasting and Hansard services.[105]

34.76 The Office of the Parliamentary Librarian is an office within the DPS. The main function of the Parliamentary Librarian is to provide information, analysis and advice to senators and members of the House of Representatives in support of their parliamentary and representational role.[106]

Submissions and consultations

34.77 In its submission, the OPC brought the ALRC's attention to this exemption. The OPC stated that, although it was not aware of any particular concerns with the exemption of the DPS, the existence of the exemption is not apparent from a reading of the *Privacy Act*. There is no reference to the exemption in either the *Privacy Act* or the *Public Service Act 1999* (Cth), from which the *Privacy Act* derives its definition of a department. The OPC suggested that 'in the interests of clarity, the exemption … should be explicitly referred to in the *Privacy Act*', and that the DPS be included in a schedule to the Act of all entities that are exempt from compliance with the Act. Furthermore, the OPC submitted that all entities that are exempt from the Act should implement a set of information-handling standards.[107]

---

102 *Parliamentary Service Act 1999* (Cth) s 54. The DPS is a Department of the Parliament established by resolutions passed by each House of the Australian Parliament: Australian Parliamentary Service Commissioner, *Annual Report 2004–05* (2005), App A.

103 Australian Parliamentary Service Commissioner, *Annual Report 2004–05* (2005), 6.

104 The Presiding Officers are the President of the Senate and the Speaker of the House of Representatives: *Parliamentary Service Act 1999* (Cth) s 7.

105 Australian Parliamentary Service Commissioner, *Annual Report 2004–05* (2005), 6.

106 *Parliamentary Service Act 1999* (Cth) ss 38A, 38B.

107 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

ALRC's view

34.78 The secondary legislative materials relating to the *Parliamentary Service Act 1999* (Cth) do not disclose a policy justification for the exemption of the parliamentary departments from the *Privacy Act*. As discussed in Chapter 30, any exemptions from the *Privacy Act* should be based on sound policy grounds and limited to the extent possible. The ALRC is interested in views on whether the parliamentary departments should continue to be exempt from the *Privacy Act*.

34.79 If there are legitimate reasons for the exemption of the parliamentary departments, the ALRC agrees with the OPC that the exemption should be referred to expressly in the *Privacy Act*. In Chapter 30, the ALRC proposes that the *Privacy Act* be amended to set out in a schedule to the Act exemptions for specific, named entities, which should distinguish between entities that are completely exempt and those that are partially exempt from the *Privacy Act*. If the exemption of the parliamentary departments were to remain, it should be included in the proposed schedule to the Act.[108]

Question 34–2 Should the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary Services continue to be exempt from the operation of the *Privacy Act*? If so, what should be the scope of the exemption?

State and territory authorities and prescribed instrumentalities

State and territory authorities

34.80 State and territory authorities fall outside the definition of an 'agency' and are also specifically excluded from the definition of an 'organisation' under the *Privacy Act*.[109] They are, therefore, exempt from the operation of the Act unless states and territories request that such authorities be brought into the regime by regulation.[110] Generally, state and territory authorities are people or bodies that are part of a state or territory public sector. They include, for example, state and territory ministers, departments, and bodies and tribunals and local governments established for a public purpose under a state or territory law.[111]

34.81 State and territory statutory corporations are excluded from the coverage of the *Privacy Act*.[112] State and territory bodies that are incorporated companies, societies or

108 Proposal 30–2.
109 *Privacy Act 1988* (Cth) ss 6(1), 6C.
110 Ibid s 6F.
111 Ibid s 6C(3).
112 Ibid s 6C(3)(c).

associations are, however, deemed to be 'organisations' for the purposes of the Act.[113] They can be prescribed out of the coverage of the Act, but only on request by the relevant state or territory and only after the minister has considered a number of issues outlined in the Act.[114]

34.82 For the period from 21 December 2001 to 31 January 2005, the OPC stated that 16% of all the NPP complaints closed by the OPC on the ground that they were outside of its jurisdiction concerned the exemption for state and local governments.[115] In 2004–05, the OPC received 2,469 enquiries concerning exemptions, of which 32% relate to state or local government bodies that are not covered by the *Privacy Act*.[116]

Prescribed state and territory instrumentalities

34.83 State and territory instrumentalities also fall outside the definition of 'agency' under the *Privacy Act*. A state and government instrumentality includes, for example, a company, society or association under the *Corporations Act 2001* (Cth).[117] They are, however, considered 'organisations' and are therefore subject to the private sector provisions of the Act, unless they have been prescribed to fall outside the definition of 'organisation' in accordance with s 6C(4) of the Act. At present, no state or territory instrumentalities have been prescribed.

34.84 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) stated that the reason for this exemption was that the acts and practices of state and territory public sector agencies are for the states and territories to regulate.[118] In addition, it was stated that:

> Sub-clause 6C(4) describes the process for making regulations that stop State or Territory instrumentalities from being organisations … One of the purposes of this sub-clause is to recognise that Commonwealth regulation of a State or Territory instrumentality (for example a Corporations Law company, society or association) that performs core government functions is inappropriate, if such regulation would curtail the capacity of the State or Territory to function as a government.[119]

---

113 Ibid s 6C(1), (3)(c)(i).

114 Ibid s 6C(4); Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 2.

115 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

116 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 38. No statistics on the number of inquiries concerning exempt state and local bodies were reported for 2005–06: see Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006).

117 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [74].

118 Ibid, notes on clauses [73].

119 Ibid, notes on clauses [74].

34.85 Some state and territory instrumentalities are required by other federal legislation to comply with the *Privacy Act*. For example, public and private sector higher education providers are required by the *Higher Education Support Act 2003* (Cth) to comply with the IPPs in respect of the personal information of students obtained for the purpose of the provision of financial assistance to students.[120]

Should state and territory authorities be exempt from the *Privacy Act*?

34.86 In submissions to the inquiry by the Senate Legal and Constitutional References Committee into the *Privacy Act* (2005 Senate Committee privacy inquiry), it was suggested that the exemption in relation to state agencies is a significant gap in the coverage of the *Privacy Act*.[121]

34.87 Another issue concerns the inconsistent coverage of state and territory entities. Some state-owned entities fall outside both federal and state privacy regimes while others are covered by both federal and state legislation. This issue is discussed in Chapter 4.[122]

Submissions and consultations

34.88 In IP 31, the ALRC asked whether state and territory authorities should be exempt from the operation of the *Privacy Act*.[123] Some stakeholders considered that state and territory authorities should be exempt from the *Privacy Act*.[124] The Office of the Information Commissioner Northern Territory submitted that:

> State and Territory authorities are the responsibility of their respective jurisdictions which should continue to be responsible for protecting the privacy of personal information collected and held by those authorities.[125]

34.89 The Victorian Office of the Health Services Commissioner stated that:

> Although it is unfortunate that certain state and territory statutory bodies fall outside both the federal and the state privacy regimes … this is not a sufficient reason for the Federal Government to attempt to regulate state and territory public sector agencies.[126]

---

120 *Higher Education Support Act 2003* (Cth) s 19-60.

121 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.38].

122 It is important to note that any action by the Australian Government to extend the *Privacy Act* to cover state and territory bodies will raise constitutional issues. This is discussed in detail in Chapter 4.

123 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–4.

124 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

125 Office of the Information Commissioner (Northern Territory), *Submission PR 103*, 15 January 2007.

126 Office of the Health Services Commissioner (Victoria), *Submission PR 153*, 30 January 2007.

34.90 In contrast, other stakeholders considered that state and territory authorities should not be exempt from the *Privacy Act*.[127] The Insurance Council of Australia submitted that removing the exemption for state and territory authorities would create the potential for conflicts between the federal and state and territory laws.[128] It was suggested in one submission that state and territory agencies should only be exempt on a case-by-case basis.[129]

34.91 Some stakeholders submitted that state and territory authorities should be exempt to the extent that they are subject to state and territory privacy laws.[130] For example, the OVPC stated that federal privacy law should not bind state authorities when they are already subject to state privacy laws, because this would result in unnecessary fragmentation and confusion. The OVPC also did not support state referral of power to the Commonwealth,

> as it would remove the state's ability to provide enhanced protection and, while dealing with the constitutional impediment, continues to suffer from the problem of how it is to interact with other state based laws (FOI, archives, human rights etc).[131]

34.92 The OVPC was, however, in favour of federal minimum standards that apply to state and territory public sectors.

> Given that not all jurisdictions have privacy laws in place, there is some merit in the proposal to have minimum standards apply to state and territory public sectors which can be 'rolled back' once that jurisdiction enacts privacy legislation that conforms to the specified federal standard—provided that this allowed for better protection to be adopted by the state and territory governments.[132]

34.93 Some stakeholders noted that the question of exemption of state and territory authorities would fall away if a uniform privacy scheme were adopted.[133]

State and territory government business enterprises

34.94 A number of statutory corporations are government business enterprises (GBEs). GBEs provide a range of services, including communications, transport, employment and health services. The three characteristics to identify GBEs are: 'the Government controls the body; the body is principally engaged in commercial activities; and the body has a legal personality separate to a department of

---

127 Insurance Council of Australia, *Submission PR 110*, 15 January 2007; Institute of Mercantile Agents, *Submission PR 101*, 15 January 2007; W Caelli, *Submission PR 99*, 15 January 2007; K Handscombe, *Submission PR 89*, 15 January 2007; I Turnbull, *Submission PR 82*, 12 January 2007.

128 Insurance Council of Australia, *Submission PR 110*, 15 January 2007.

129 K Pospisek, *Submission PR 104*, 15 January 2007.

130 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007; Australian Privacy Foundation, *Submission PR 167*, 2 February 2007.

131 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

132 Ibid.

133 Queensland Government, *Submission PR 242*, 15 March 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

government'.[134] A state or territory GBE may be a body corporate established by legislation for a public purpose (state-owned or statutory corporations), or a company established under corporations law in which a state or territory government has a controlling interest.

34.95 Currently, there is inconsistent coverage of state and territory statutory corporations under state and territory privacy laws. For example, statutory corporations are covered by privacy legislation in Victoria but not in New South Wales.[135] In Tasmania, specified statutory authorities that are GBEs are covered by privacy legislation.[136] The exemption for statutory corporations in New South Wales (NSW) was originally provided on the basis that statutory corporations should not be put at a competitive disadvantage with the private sector. The then Attorney General of NSW, the Hon Jeff Shaw, stated that:

> When the Act evolves to include coverage of the private sector, State-owned corporations will be similarly covered by the information and privacy principles of the legislation. The Government intends to address this issue in detail following the March 1999 election.[137]

34.96 NSW legislation has not yet been amended to cover statutory corporations.

Submissions and consultations

34.97 Particular concern was raised in submissions that some state-owned statutory corporations are excluded from both the state and the federal privacy regimes.[138] Some stakeholders considered that government businesses that compete with private sector organisations should be subject to the *Privacy Act*.[139]

34.98 In its submission, the OPC made a distinction between departments of state and agencies responsible for direct implementation of government policy, and state and territory entities incorporated for a public purpose by or under law. The OPC was of the view that

---

134 Administrative Review Council, *Report to the Minister of Justice: Government Business Enterprises and Commonwealth Administrative Law*, Report 38 (1995), 7.

135 The *Information Privacy Act 2000* (Vic) applies to 'public sector agency', ie, a public service body or a public entity within the meaning of the *Public Administration Act 2004* (Vic): *Information Privacy Act 2000* (Vic) ss 3, 9(1)(c). Under the *Public Administration Act*, public entities include bodies that are established by or under an Act (other than a private Act) or the Corporations Act: *Public Administration Act 2004* (Vic) s 5.

136 The *Personal Information Protection Act 2004* (Tas) applies to 'public sector body', which is defined to include GBEs under the *Government Business Enterprises Act 1995* (Tas).

137 New South Wales, *Parliamentary Debates*, Legislative Council, 25 November 1998, 10592 (J Shaw—Attorney General).

138 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006.

139 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

> the acts and practices of state and territory bodies that are responsible for policy development and implementation, and for the making of laws, should generally be subject to the oversight of the respective Parliament, and thus ultimately accountable to the electorate of that jurisdiction. This includes Ministers and departments of state in those jurisdictions and bodies, as well as bodies established for a public purpose by or under a law of that state or territory.[140]

34.99 The OPC submitted, however, that state-owned statutory corporations that function as government businesses should be covered by the *Privacy Act*, because not all states and territories have enacted privacy legislation, and the lack of privacy protection for personal information handled by statutory corporations may be inconsistent with community expectations. Furthermore, it submitted that 'applying privacy regulation to state and territory statutory corporations is likely to be consistent with the principle of competitive neutrality'.[141] On this basis, the OPC suggested a three-pronged approach, involving:

- the Australian Government working with all states and territories to implement privacy regulation that is consistent with the *Privacy Act* or adopt the *Privacy Act* as model legislation;

- the application of the *Privacy Act* to all incorporated bodies, including state and territory statutory corporations, except where there is equivalent privacy legislation in the relevant jurisdiction; and

- where it is considered necessary, that state and territory incorporated bodies exempted from coverage of the *Privacy Act* on public interest grounds, by applying a provision such as s 6C(4) of the Act to give effect to the exemption.[142]

34.100 Similarly, Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that:

> There is no reason why State or Territory business enterprises should have an arguable commercial advantage over private sector organisations because they can avoid the costs of compliance with privacy laws. On the other hand, there is no reason why the Commonwealth should monopolise power to establish appropriate privacy standards. Consistency in privacy standards across Australia is desirable, but that is a separate issue. The best balance is struck simply by ensuring that some enforceable privacy standard applies …

---

140 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

141 National Competition Council, *Compendium of National Competition Policy Agreements* (1998), cl 3.

142 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

> The law should make provision for coverage of any state or territory authorities 'by agreement' (effected through Regulations) to cover the increasing number of 'hybrid' organisations involved in the delivery of public services and to ensure no organisation can 'fall between the gaps'.[143]

34.101 Other state and territory bodies that have been suggested for coverage under the *Privacy Act* include:

- bodies established by administrative arrangements, including on a cooperative basis between jurisdictions; [144]
- universities established under state or territory legislation;[145] and
- federally funded state entities, such as hospitals, research institutes, universities, schools, environment management agencies and road authorities.[146]

34.102 Some stakeholders submitted that certain state and territory bodies should continue to be exempt from the operation of the *Privacy Act*.[147] The NSW Guardianship Tribunal submitted that state and territory guardianship tribunals should remain exempt.[148] The Australian Guardianship and Administration Committee submitted that public trustees should be exempt 'from appropriate provisions of the *Privacy Act* … where the Public Trustee is seeking information about a person, from either the private or public sector, in the ordinary course of the Public Trustee's business as trustee'.[149]

Opt-in provision

34.103 Under s 6F of the *Privacy Act*, state and territory governments may request that certain state and territory authorities or instrumentalities be treated as organisations under the Act. One of the purposes of this opt-in provision

> is to allow statutory corporations whose activities are predominantly commercial, to 'opt-in' to the private sector privacy regime where the State (or Territory) and Minister (in consultation with the Privacy Commissioner) consider that it is appropriate to do so.[150]

---

143 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183*, 9 February 2007.

144 Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

145 Ibid; D Antulov, *Submission PR 14*, 28 May 2006.

146 I Turnbull, *Submission PR 82*, 12 January 2007.

147 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007; Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

148 New South Wales Guardianship Tribunal, *Submission PR 209*, 23 February 2007.

149 Australian Guardianship and Administration Committee, *Submission PR 129*, 17 January 2007.

150 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [96].

34.104 At present, only four state-owned entities have been brought into the federal privacy regime by regulation—Country Energy, EnergyAustralia, Integral Energy Australia and Australian Inland Energy Water Infrastructure.[151]

34.105 In IP 31, the ALRC asked whether any other state and territory authorities should be covered by the privacy principles in the *Privacy Act*, and if so to what extent they should be covered.[152] The OVPC suggested that the opt-in mechanism in s 6F of the *Privacy Act* should remain, because 'while it appears not to have been used, it may be in the future and this type of mechanism maintains control by and independence of the states'. [153]

Options for reform

34.106 Particular concerns have been raised in submissions about the inconsistent coverage of some state and territory GBEs by state and territory privacy laws. Any proposal to bring GBEs under the *Privacy Act*, however, must take into account the fact that some of them are already subject to state or territory privacy law. To avoid subjecting these bodies to two sets of privacy laws, there are essentially two options for reform.

34.107 One option is to provide that state and territory authorities be covered by the *Privacy Act* unless they are covered by a state or territory law that is 'substantially similar' to the *Privacy Act*. In Canada, s 26(2)(b) of the *Personal Information Protection and Electronic Documents Act* (2000) (Canada) provides that the Governor in Council may,

> if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.[154]

34.108 The Privacy Commissioner of Canada has determined that, in assessing whether provincial legislation is 'substantially similar' to the federal legislation, the Commissioner would

> interpret substantially similar as equal or superior to the [*Personal Information Protection and Electronic Documents Act*] in the degree and quality of privacy

---

151 *Privacy (Private Sector) Regulations 2001* (Cth) reg 3A. Australian Inland Energy Water Infrastructure was subsequently dissolved in July 2005: *Energy Services Corporation (Dissolution of Australian Inland Energy Water Infrastructure) Regulation 2005* (NSW).

152 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–4.

153 Office of the Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007.

154 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 26(2)(b).

> protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.[155]

34.109 Another option is to model the provision on s 18BB(2)(a) of the *Privacy Act*. Section 18BB(2) provides that, before the Privacy Commissioner approves a privacy code, the Commissioner must be satisfied of a number of matters. One of these matters is that 'the code incorporates all the National Privacy Principles or sets out obligations that, overall, are at least the equivalent of all the obligations set out in those Principles.'

34.110 The OPC's *Guidelines on Privacy Code Development* provide guidance on how the Privacy Commissioner assesses whether the condition in s 18BB(2)(a) is met.

> In deciding if this condition has been met, the Commissioner requires code proponents to include a statement of claims detailing:
>
> i) how the obligations under the code differ from the obligations under the NPPs;
>
> ii) the rationale for the change to any obligation provided in the NPPs; and
>
> iii) how, in the opinion of the code proponent, the obligations set out in the code are at least equivalent of all the obligations set out in the NPPs.[156]

ALRC's view

34.111 Concerns have been raised in submissions about the inconsistent coverage of state and territory authorities under state and territory laws. The exemption of these authorities from the operation of the *Privacy Act* means that only those state and territory authorities that are subject to state and territory privacy laws are covered by privacy regulation. The exemption of state and territory authorities represents a significant gap in privacy regulation in Australia.

34.112 Particular concerns were raised about the exemption of state-owned statutory corporations that compete with private sector organisations. In the ALRC's view, the exemption of state-owned statutory corporations from the *Privacy Act* is not justified where they are in competition with an organisation and not subject to equivalent obligations under state or territory privacy legislation. State-owned statutory corporations that compete with private sector organisations should not have a competitive advantage.

34.113 In Chapter 4, the ALRC proposes that state and territories enact legislation applying the proposed Unified Privacy Principles and the proposed *Privacy (Health Information) Regulations* to the state and territory public sector agencies.[157] The enactment of such legislation would resolve issues concerning inconsistent regulation of state and territory authorities. The implementation of such a scheme, however, is likely to take time.

---

155 Privacy Commissioner of Canada, *Report to Parliament Concerning Substantially Similar Legislation* (2002), 2.

156 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001).

157 Proposal 4–4.

34.114 The ALRC is of the view that, before the proposed enactment of similar legislation in the state and territories, the *Privacy Act* should be amended to apply to all state and territory incorporated bodies, including statutory corporations, except where: they are covered by state or territory privacy law setting out obligations that, overall, are at least the equivalent of the relevant obligations in the *Privacy Act*; or the minister is satisfied that they should be exempt on public interest grounds.

34.115 The ALRC considers that the approach in considering whether a state or territory has equivalent privacy laws should be modelled on s 18BB(2)(a) of the *Privacy Act*. This option is preferable to the Canadian approach because the Privacy Commissioner already has experience in assessing equivalence under s 18BB(2)(a).

34.116 Currently, s 6C(4) of the *Privacy Act* provides a mechanism for regulations to be made to exclude a state or territory instrumentality from the coverage of the Act. In summary, s 6C(4) provides that, before exempting a state or territory instrumentality, the minister must: be satisfied that the exemption is requested by the state or territory; consider whether coverage of the body under the *Privacy Act* would adversely affect the state or territory government; the desirability of regulating that body under the *Privacy Act*; whether there are equivalent privacy laws that apply to that body; and consult with the Privacy Commissioner. The adoption of this mechanism would ensure that those state and territory bodies that should be exempt on public interest grounds, for example, because they are involved in policy development and implementation rather than in competition with organisations, are exempt from the *Privacy Act*.

Proposal 34–5 Subject to Proposal 4–4 (states and territories to enact legislation applying the proposed Unified Privacy Principles and *Privacy (Health Information) Regulations*), the *Privacy Act* should be amended to:

(a) apply to all state and territory incorporated bodies, including statutory corporations, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of the relevant obligations in the *Privacy Act*; and

(b) empower the Governor-General to make regulations exempting state and territory incorporated bodies from coverage of the *Privacy Act* on public interest grounds.

Proposal 34–6 The *Privacy Act* should be amended to provide that, in considering whether to exempt state and territory incorporated bodies from coverage of the *Privacy Act*, the Minister must:

(a) be satisfied that the state or territory has requested that the body be exempt from the Act;

(b) consider:

(i) whether coverage of the body under the *Privacy Act* adversely affects the state or territory government;

(ii) the desirability of regulating under the *Privacy Act* the handling of personal information by that body; and

(iii) whether the state or territory law regulates the handling of personal information by that body to a standard that is at least equivalent to the standard that would otherwise apply to the body under the *Privacy Act*; and

(c) consult with the Privacy Commissioner about the matters mentioned in paragraphs (ii) and (iii) above.

35. Small Business Exemption

Contents

Introduction 1007
Current law 1007
Retention of the exemption 1010
Costs of compliance 1012
Consent provisions 1014
Submissions and consultations 1014
Removal of the exemption 1019
Definition of 'small business' 1022
High risk sectors 1026
Modifying the application of the privacy principles to small businesses 1032
EU adequacy and implementation of the APEC Privacy Framework 1033
Voluntary compliance and opting in 1035
ALRC's view 1036

Introduction

35.1 Generally speaking, small businesses—namely, those that have an annual turnover of $3 million or less—are exempt from the operation of the *Privacy Act 1988* (Cth).[1] It has been estimated that up to 94% of businesses may fall under this exemption. This exemption has been the subject of a number of criticisms and scrutinised by four separate inquiries since 2000.[2] This chapter examines whether the exemption should be retained or removed, and sets out the ALRC's proposals to reform the exemption.

Current law

35.2 Under s 6C of the *Privacy Act*, a small business operator is specifically excluded from the definition of 'organisation' and generally is exempt from the operation of the

1 *Privacy Act 1988* (Cth) s 6C.

2 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000); Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

Act. A 'small business operator' is an individual, body corporate, partnership, unincorporated association or trust that carries on one or more small businesses, and does not carry on a business that is not a small business.[3]

35.3 A 'small business' is a business that has an annual turnover of $3 million or less in the previous financial year (or in the current financial year if it is a new business).[4] 'Small businesses' can include non-profit bodies and unincorporated associations,[5] even though the ordinary meaning of the term 'business' may not include such bodies. There are a number of conditions that qualify the application of the exemption for small businesses. A small business may still be covered by the *Privacy Act* if it:

- provides a health service and holds personal health information except in an employee record;[6]
- collects personal information about another individual from, or discloses such information to, anyone else for benefit, service or advantage (unless it always has the consent of the individuals concerned, or only does so when authorised or required by law);[7]
- is or was contracted to provide services to the Australian Government or its agencies;
- is related to a larger business;
- is prescribed by regulation; or
- elects to 'opt in' to be treated as if it were an 'organisation' within the meaning of the *Privacy Act*.[8]

---

3 *Privacy Act 1988* (Cth) s 6D(3).

4 Ibid s 6D(1). The annual turnover of a business for a financial year includes the proceeds of sales of goods and/or services; commission income; repair and service income; rent, leasing and hiring income; government bounties and subsidies; interest, royalties and dividends; and other operating income earned in the year in the course of business: *Privacy Act 1988* (Cth) s 6DA. It does not include assets held by small businesses, capital gains or proceeds of capital sales: Office of the Privacy Commissioner, *A Privacy Checklist for Small Business* <www.privacy.gov.au/business/small/index.html> at 1 August 2007.

5 Office of the Privacy Commissioner, *A Snapshot of the Privacy Act for Small Business* <www.privacy.gov.au/business/small/bp.html> at 1 August 2007.

6 Examples of health service providers that hold personal health information not contained in an employee record include medical practices, pharmacies and health clubs: Australian Government Attorney-General's Department, *Fact Sheet on Privacy in the Private Sector—Small Business* (2000) <www.ag.gov.au> at 1 August 2007. An 'employee record' is defined to mean a record of personal information relating to the employment of the employee: *Privacy Act 1988* (Cth) s 6(1).

7 *Privacy Act 1988* (Cth) s 6D(7), (8). See also Office of the Privacy Commissioner, *What Does 'Trading in Personal Information' Mean?* <www.privacy.gov.au/faqs/sbf/q2.html> at 1 August 2007.

8 *Privacy Act 1988* (Cth) ss 6D(4), (9), 6E, 6EA.

35.4 In addition, under s 6E(1A) of the *Privacy Act*, a small business operator that is a 'reporting entity'—ie, a person who provides a 'designated service' under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)[9]—is deemed to be an 'organisation' for the purposes of the *Privacy Act*. This provision was enacted to bring small business operators under the jurisdiction of the *Privacy Act* in relation to their obligations to collect personal information for the purposes of compliance with anti-money laundering and counter-terrorism financing legislation.

35.5 The Attorney-General may prescribe that certain small businesses or their activities be subject to the Act. The Attorney-General may do so if it is in the public interest and after consultation with the Privacy Commissioner.[10] This provision is intended to enable otherwise exempt businesses to be brought within the federal privacy scheme if they are found to constitute a particular risk to individual privacy.[11]

35.6 The Office of the Privacy Commissioner (OPC) keeps a register of those businesses that choose to 'opt in'. Currently there are 168 small businesses that have opted to be covered by the *Privacy Act*.[12]

35.7 When the private sector amendments were enacted, small businesses were exempted on the basis that many of them do not pose a high risk to privacy.[13] The Australian Government took the view that many small businesses do not have significant holdings of personal information, and those that may have customer records do not sell or otherwise deal with customer information in a way that poses a high risk to their customer's privacy.[14]

35.8 It was also the policy of the Australian Government to minimise compliance costs on small businesses.[15] The specified conditions that qualify the application of the small business exemption were intended to acknowledge that some personal information and some activities pose a higher risk to privacy than others, and that small businesses within these categories ought to be covered by the Act.[16]

---

9 'Designated services' include a number of specified financial, bullion trading or gambling services, as well as services prescribed by regulation: *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 6.

10 *Privacy Act 1988* (Cth) s 6E(4).

11 Australian Government Attorney-General's Department, *Fact Sheet on Privacy in the Private Sector—Small Business* (2000) <www.ag.gov.au> at 1 August 2007.

12 Office of the Privacy Commissioner, *Opting-In to Coverage by the National Privacy Principles* <www.privacy.gov.au/business/register/index.html> at 1 August 2007.

13 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.

14 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General), 22370–22371.

15 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.

16 Ibid, 6.

35.9 For the period from 21 December 2001 to 31 January 2005, 20% of all the National Privacy Principles (NPPs) complaints closed by the OPC as outside of its jurisdiction concerned the small business exemption.[17] In 2005–06, the OPC received 2,000 enquiries concerning exemptions, of which 21% relate to the small business exemption.[18]

35.10 There are no provisions for an exemption for small businesses in international privacy instruments—namely, the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development, the European Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[19] There also are no similar exemptions in comparable jurisdictions, such as the United Kingdom, Canada and New Zealand.[20]

Retention of the exemption

35.11 The small business exemption was introduced in the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Privacy Amendment (Private Sector) Bill was the subject of two parliamentary committee inquiries—the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry (2000 House of Representatives Committee inquiry)[21] and the Senate Legal and Constitutional Legislation Committee inquiry (2000 Senate Committee inquiry).[22]

35.12 Despite noting a number of criticisms of the small business exemption, the 2000 House of Representatives Committee inquiry took the view that an effective regulatory balance must be achieved in order to avoid overburdening small businesses that pose a low privacy risk, and that this cannot be achieved without some form of exemption for small businesses.[23] The 2000 Senate Committee inquiry recommended the retention of the exemption, on the basis that it 'achieve[s] an adequate balance between concerns

---

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

18 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 27.

19 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

20 *Data Protection Act 1998* (UK); *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada); *Privacy Act 1993* (NZ).

21 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000).

22 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000).

23 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.16].

about the coverage of the exemption and the intention not to impose too great a burden on small businesses'.[24]

35.13 In 2005, both the OPC and the Senate Legal and Constitutional References Committee reviewed the private sector provisions of the *Privacy Act*.[25] Submissions to the review by the OPC of the private sector provisions of the *Privacy Act* (OPC Review) were roughly divided between retention of the small business exemption and its repeal.[26] In evidence before the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (2005 Senate Committee privacy inquiry), the Privacy Commissioner did not recommend the abolition of the exemption because:

> One of the premises of the [A]ct is that there be a balance between the individual's right to privacy and the community's needs, and between the free flow of information and businesses operating efficiently. If the small business exemption were removed entirely, there would be a cost to I think it is 1.2 million small businesses in Australia.[27]

The Privacy Commissioner acknowledged, however, that the OPC had not assessed the estimated cost of removing the exemption.[28]

35.14 The 2005 Senate Committee privacy inquiry questioned the need to retain the small business exemption. It considered that privacy rights of individuals should be protected regardless of whether they are dealing with a small business, and that protecting these rights also makes commercial sense for all businesses. Given that privacy regimes in some overseas jurisdictions have operated effectively without the exemption, and that the existence of the exemption is one of the key outstanding issues preventing recognition of Australian privacy laws under the EU Directive,[29] the inquiry recommended that the small business exemption be removed from the *Privacy Act*.[30]

35.15 In response to questions during the 2005 Senate Committee privacy inquiry as to whether it was still necessary or desirable to achieve European Union (EU) adequacy given the use of contractual privacy standards by most businesses, the Privacy

---

24 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.11]–[3.12].

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

26 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 180.

27 Commonwealth, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 49 (K Curtis—Privacy Commissioner).

28 Ibid.

29 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

30 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32]–[7.34], rec 12.

Commissioner stated that it would be simpler for businesses if they did not have to use contractual privacy provisions.[31]

35.16 According to the Australian Government Attorney-General's Department, the small business exemption appears to be the 'key outstanding issue' as to how the matter of EU adequacy is to be resolved between the European Union and Australia.[32] As noted above, this was one of the reasons the 2005 Senate Committee privacy inquiry recommended that the small business exemption be removed from the *Privacy Act*.[33]

35.17 The 2005 Senate Committee privacy inquiry recommended that the ALRC investigate possible measures that could assist Australia in achieving EU adequacy.[34] The Australian Government disagreed with this recommendation, on the basis that 'international negotiations are a matter for the Australian Government and negotiations with the European Union are ongoing'.[35] It is the ALRC's understanding that negotiations with the EU on this issue are ongoing. The issue of EU adequacy is discussed further in Part J.

35.18 In its response to the OPC Review and the 2005 Senate Committee privacy inquiry, the Australian Government has indicated that it 'supports the retention of the small business exemption',[36] and that

> the small business exemption strikes an appropriate balance between the risk of privacy breaches and over regulation of small businesses. Removal of the exemption would be inconsistent with the Government's commitment to workplace reform and cutting red tape.[37]

Costs of compliance

35.19 If the small business exemption were removed, compliance costs could include the costs of: obtaining legal advice; educating or training staff on privacy requirements; maintaining security of personal information held; and dealing with requests from customers for access to and correction of their personal information. Many of these costs may be ongoing.

---

31 Ibid, [4.136]. The use of contractual privacy provisions to facilitate trade with EU organisations is discussed in Ch 13.

32 Ibid, [4.139].

33 Ibid, [7.33]–[7.34], rec 12.

34 Ibid, rec 16.

35 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006), 5.

36 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 10.

37 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006), 4.

35.20 Business has identified privacy requirements as an important contributor to their cumulative regulatory burden. In its 2006 report, *Rethinking Regulation*, the Productivity Commission's Taskforce on Reducing Regulatory Burdens on Business recommended that the Australian Government consider the impact of privacy requirements on business compliance costs in the context of a wider review of Australian privacy laws.[38]

35.21 In its 2006 report, *The Victorian Regulatory System*, the Victorian Competition and Efficiency Commission noted the challenge for government in assisting small businesses in complying with regulation, 'given the need to provide adequate protection to the consumers of products produced by these businesses, as well as their workers and the environment'.

> There are a number of ways of meeting this challenge. In some cases, there may be less onerous provisions in the regulations which relate to small businesses … or even exemptions … However, such approaches by favouring some businesses over others can distort markets, and discourage smaller businesses growing past such thresholds. Another approach, advocated by the United Kingdom's Better Regulation Taskforce was to 'think small first' based on the assumption that regulation designed with the capacity and constraints of small business in mind would also be readily implemented by larger businesses.

35.22 The Commission went on to note that 'another approach is to have a consistent regulatory system but to provide special assistance for smaller businesses'.[39]

35.23 The Australian Chamber of Commerce and Industry (ACCI) argued that the low risk to privacy posed by small businesses and the potentially high compliance costs are reasons to retain the small business exemption.[40]

35.24 Associate Professor Moira Paterson provides a counter to this argument when she notes that the costs of compliance on businesses are likely to be significant only where businesses have poor record-keeping practices. Paterson noted that there was evidence from Quebec that implementing data protection measures may in fact result in cost reduction or increased productivity due to improved information-handling practices.[41] Furthermore, she observed that, in New Zealand,

> the limited information available to date does not suggest that the cost of implementation has been a major problem. For example, the New Zealand Real Estate Institute commented in 1994 that, while the passing of the Privacy Act 1993 (NZ) would have a considerable impact on the manner in which the industry might deal

---

38 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), rec 4.48.

39 Victorian Competition and Efficiency Commission, *The Victorian Regulatory System* (2006), 26–27.

40 Australian Chamber of Commerce and Industry, 'Privacy Act Review Must Not Add to Small Business Compliance Costs' (2005) 119 *ACCI Review* 1, 3.

41 M Paterson, 'Privacy Protection in Australia: The Need for an Effective Private Sector Regime' (1998) 26 *Federal Law Review* 372, 383, 399.

with personal information, it did not expect that there would be any significant cost of compliance; what was required was common sense and fair dealing.[42]

Consent provisions

35.25 At present, a small business that trades in personal information may still be exempt if it has the consent of the individuals concerned to collect or disclose their personal information.[43] The OPC Review recommended the removal of the consent provision on the basis that the provision is 'clumsy and complicated', and that there is a lack of certainty as to whether a single failure to gain consent would change the exempt status of the business.[44] In the OPC's view, this would also ensure that all organisations that trade in personal information would be regulated by the *Privacy Act*, and that public number directory producers cannot make use of the exemption.[45]

35.26 In its response to the OPC Review, the Australian Government disagreed with the OPC Review's recommendation on the basis that 'the Act currently provides a mechanism for dealing with situations in which the consent provisions should not operate'.[46]

Submissions and consultations

35.27 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the small business exemption should remain, and if so, what should be its extent.[47] Some stakeholders considered that the small business exemption should be retained.[48] A number of submissions emphasised the need to balance privacy protection and the interest of the business sector to operate efficiently.[49] Two main reasons were

---

42 Ibid, 399.

43 *Privacy Act 1988* (Cth) s 6D(7), (8).

44 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 185, rec 53.

45 Ibid, 62, 185. Public number directory producers are authorised to access data concerning listed telephone numbers from the Integrated Public Number Database, a database of all listed and unlisted public telephone numbers in Australia: Australian Government Department of Communications Information Technology and the Arts, *Integrated Public Number Database (IPND)* <www.dcita.gov.au/communications_and_technology/policy_and_legislation/numbering> at 1 August 2007. Public number directory producers are persons who: (i) compile, publish, maintain or produce directories of public numbers; (ii) provide directory assistance services; or (iii) supply goods or services which are a combination of (i) and (ii): Australian Communications Authority, *Telecommunications (Section of the Telecommunications Industry) Determination*, 25 September 1998.

46 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 10.

47 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–6.

48 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

49 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Council of Small Business Organisations of Australia Ltd, *Submission PR 203,* 21 February 2007 (which supported the submission lodged by Real Estate Institute of Australia, as one of its members); Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

suggested as to why the exemption should be retained, namely, that: small businesses pose a low risk to privacy because many small businesses do not collect a significant amount of personal information or deal inappropriately with personal information;[50] and the removal of the exemption would increase the overall regulatory burden and compliance costs.[51] One stakeholder also suggested that 'the consequences of misuse of personal information by small business will generally be less than misuse by large organisations or government'.[52]

35.28 The OPC stated that the small business exemption is 'necessary to balance privacy protection against the need to avoid unnecessary cost on small business'. It cited research undertaken by the Regulation Taskforce, which showed that compliance matters can consume up to 25% of the time of large companies and that the impact would be even greater for small businesses that generally do not have the in-house capacity to keep abreast of large amounts of regulation.[53] The OPC conceded, however, that the exemption

> may not promote consistency and may lead to additional burdens for small businesses and individuals because of the uncertainty it creates about whether personal information is regulated by the *Privacy Act*. … For individuals there may be an expectation that their personal information will be regulated by the NPPs and there may not be sufficient awareness that consent given to a small business could mean this protection is not provided.[54]

35.29 The OPC also noted that, under s 6E(1A) of the *Privacy Act*,

> personal information held by small businesses will only be covered [by the Act] where it has been collected for the purposes of anti-money laundering and counter-terrorism financing regulation. Accordingly, relevant small business will need to be able to distinguish between personal information that is regulated, and that which is not. The Office considers that many small business reporting entities may find that compliance is simplified by treating all personal information as though it is covered by the Privacy Act.[55]

---

50 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Council of Small Business Organisations of Australia Ltd, *Submission PR 203,* 21 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

51 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Council of Small Business Organisations of Australia Ltd, *Submission PR 203,* 21 February 2007; Communications Alliance Ltd, *Submission PR 198,* 16 February 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

52 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

53 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007, referring to Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), ii.

54 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007, referring to Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), ii.

55 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

35.30 Consistent with its recommendation in the OPC Review, the OPC further submitted that the consent provisions in ss 6D(7) and 6D(8) of the *Privacy Act* should be clarified as to whether a single failure by a small business to gain consent of an individual to trade in his or her personal information would affect the exempt status of that small business.[56]

35.31 Some stakeholders considered that the exemption should be retained because there are already mechanisms in the *Privacy Act* that limit the application of the exemption: by excluding those small businesses that engage in activities that pose a high risk to privacy; or those that enter into certain business relationships, for example, with government or larger organisations.[57]

35.32 The Victorian Automobile Chamber of Commerce (VACC) submitted that the exemption has been advantageous to its members in reducing the cost of compliance with the Act. VACC stated that the key concern raised by members that operate small businesses was that 'time would be taken away from the core business activities in order to comply with the privacy requirements, reducing their ability to be competitive or make a profit'.[58]

35.33 The Real Estate Institute of Australia (REIA) suggested that:

> Australian small businesses do in fact attract a relatively low number of privacy complaints after considering the sheer number of small businesses, their share of total sales of good and services and the likelihood that complaints outside the jurisdiction of the OPC may actually relate to a host of alternative exemptions.[59]

35.34 Some stakeholders expressed the view that small businesses already take steps to ensure that the personal information of customers is handled appropriately.[60] The VACC suggested that 'reputation and repeat business are essential for small businesses to survive. It is therefore in their best interests to handle information appropriately'.[61]

35.35 The ACCI, REIA and VACC suggested that the current threshold of $3 million is too low. Both the ACCI and the REIA submitted that the threshold for the small business exemption should be increased to an annual turnover of $5 million.[62] The REIA suggested that the threshold for the exemption should be raised to $5 million 'in order to reflect the ongoing impact of inflation and the recent period of economic

---

56 Ibid.

57 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

58 Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

59 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

60 Australian Retailers Association, *Submission PR 131,* 18 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

61 Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

62 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

prosperity that is likely to have lifted the annual turnover of many small businesses', and that this would ensure that the threshold may be left unchanged over the short term.[63] The VACC submitted that, in 2004:

> small businesses within the automotive industry estimated an annual turnover of approximately $6–7 million despite recording minimum profit margins. Given the high cost of vehicles which are generally greater than $20,000, it is not difficult for small businesses to exceed the $3 million threshold.[64]

35.36 Two stakeholders suggested that the threshold for determining what is a small business must be periodically reviewed and updated to ensure that it remains contemporary and relevant.[65] The REIA submitted that this could be done by locating the small business exemption in regulations.[66]

Costs of compliance

35.37 In submissions to this Inquiry, a number of stakeholders suggested that, if the small business exemption were removed, the costs of compliance would be significant.[67] The costs of compliance would include costs relating to: obtaining advice from external sources, such as legal advice;[68] training and educating staff;[69] purchasing and maintaining reporting and information technology systems;[70] obtaining consent from individuals for the collection and use of the information in business activities;[71] keeping information up-to-date;[72] maintaining security of personal information held;[73] handling access and correction requests;[74] staff members being allocated the role of privacy officers;[75] management and staff time for implementation, reporting and training;[76] and lost business opportunities in circumstances where restrictions on the use of information precludes normal activities.[77] The ACCI suggested that ongoing

---

63 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
64 Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.
65 Council of Small Business Organisations of Australia Ltd, *Submission PR 203,* 21 February 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
66 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
67 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; AXA, *Submission PR 119,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007
68 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
69 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
70 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
71 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
72 Ibid.
73 Ibid.
74 Ibid.
75 Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.
76 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
77 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

compliance costs would also include 'implementation of the policy, staff training, updating of the policy and dealing with inevitable complaints (legitimate or otherwise)'.[78]

35.38 The ACCI submitted that the total fixed costs to establish a simple privacy regime for an individual business would be $3,500. It stated that:

> Estimates of the legal costs for drafting a rudimentary privacy policy in 2007, though again tempered by the fact that the cost could vary considerably depending upon the characteristics of the business, were approximated at $2500. Supporting documentation, in terms of reference material such as the *Federal Privacy Handbook* and the *Privacy [Compliance] Toolkit* would now cost an additional $1000.[79]

35.39 It was noted that small businesses feel the impact of regulation more keenly than large businesses.[80] The ACCI suggested that this is because small businesses: have a narrower revenue base over which to spread the fixed costs of compliance; may not have in-house regulatory expertise to assist with compliance; may lack the time to keep abreast of regulatory developments; and may be discouraged by the complexity of regulation and the threat of penalties for even inadvertent non-compliance. The ACCI was of the view that regulation also can cause businesses to adjust their processes in ways that add to costs, and can make some commercial pursuits unviable or less attractive.[81]

35.40 The REIA suggested that the Australian Government should publish an analysis of the potential costs of abolishing the small business exemption. It submitted that:

> unnecessarily subjecting low risk businesses to the Privacy Act 1988 would simply add to the total regulatory burden and drive up costs without resulting in any significant additional protection for Australian consumers at large.[82]

35.41 On the other hand, it was suggested that any compliance costs would be proportional to the business size—if business operations were small, the costs of compliance would be low.[83] The view was expressed that there are many ways to reduce unnecessary costs of compliance without having an exemption, such as providing small businesses with guidance on records management and collection.[84] For example, the Government of South Australia submitted that:

> as many small businesses do not have significant holdings of personal information, the effect of removing the exemption on the cost burden of compliance is not expected to be significant … Minimising compliance costs should focus on unnecessary compliance cost, not compliance cost per se. There may be different ways and means to minimize unnecessary compliance costs, such as effective

78 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
79 Ibid.
80 Ibid; AXA, *Submission PR 119,* 15 January 2007.
81 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
82 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
83 Government of South Australia, *Submission PR 187,* 12 February 2007.
84 Ibid.

> business awareness raising, more detailed and practical guidance from relevant government agencies, particularly the Office of the Federal Privacy Commissioner (through provision of sample privacy policies, manuals and training kits).[85]

35.42 Abacus–Australian Mutuals (Abacus), while supportive of the extension of the NPPs to small businesses, submitted that any reform of the exemption should be subject to appropriate consultation with affected industries and industry bodies to consider compliance and implementation issues to ensure that compliance costs were not substantive.[86]

Removal of the exemption

35.43 There have been a number of criticisms of the small business exemption. Professor Graham Greenleaf argues that consumers may not be able to determine with any certainty whether the small business exemption applies to the business they are dealing with.[87] He contends that the exemption operates unfairly to prejudice the interests of small businesses that wish to protect privacy, and is so broad as to undermine the credibility of the Act.[88] He further argues that the small business exemption contains a loophole that allows the operator of a number of small businesses to engage in unrestricted transfer and use of personal information, when those small businesses have a combined turnover exceeding $3 million.[89] Similarly, Nigel Waters argues that, together with the exemption for related bodies corporate,[90] the small business exemption may allow large organisations to transfer their data collection activity to a smaller entity within their corporate structure.[91]

35.44 Other arguments for removal of the exemption include, that: there is no appropriate criteria that could exempt only those small businesses that pose low risk to privacy, because any definition of 'small business' would be arbitrary; some small businesses, especially those in high risk sectors, handle large amounts of personal information and carry out some of the most privacy intrusive activities; the compliance burden can be minimised by modifying the application of the privacy principles to small businesses without an exemption; and removal of the exemption would facilitate trade with EU organisations.

---

85 Ibid.

86 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

87 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 4.

88 Ibid, 4.

89 Ibid, 5.

90 An act or practice is not an interference with privacy if it consists of the collection or disclosure of non-sensitive personal information by a body corporate from or to a related body corporate: *Privacy Act 1988* (Cth) s 13B(1). The exemption for related bodies corporate is discussed below.

91 N Waters, 'Australian Privacy Laws Compared: "Adequacy" under the EU Data Protection Directive? Pt 2—Telecommunications and Private Sector' (2001) 8 *Privacy Law & Policy Reporter* 39.

Submissions and consultations

35.45 In submissions, there was strong support for the removal of the small business exemption.[92] A number of stakeholders expressed concern that the exemption effectively removes 94% of all businesses from the protection afforded to individuals under the *Privacy Act*.[93] The fact that a substantial number of all NPP complaints closed by the OPC were as a result of the complaints being outside the OPC's jurisdiction due to the small business exemption was also cause for concern.[94] The Office of the Victorian Privacy Commissioner stated that:

> About 30% of our enquiries result in referrals to the federal Office of the Privacy Commissioner, and the majority of these relate to small businesses which are likely to be exempt under the federal Act.[95]

35.46 Some stakeholders submitted that the protection of privacy rights should not depend on the size of business.[96] A view was also expressed that the ability of a business to misuse personal information is not related to its size, and that the consequences of misuse by small businesses could be just as severe as those for larger businesses.[97] Another stakeholder submitted that if individuals want their private personal information protected, they would have to choose to deal with businesses that have an annual turnover of more than $3 million.[98]

35.47 It was noted in a number of submissions that the assumption that small businesses are unlikely to hold significant amounts of personal information, or that they are unlikely to deal with it inappropriately, may no longer be valid.[99] Some small businesses do in fact hold large amounts of personal information, for example, internet

---

92 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; ACTU, *Submission PR 155,* 31 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

93 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

94 Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

95 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

96 Ibid; Government of South Australia, *Submission PR 187,* 12 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

97 ACTU, *Submission PR 155,* 31 January 2007.

98 I Turnbull, *Submission PR 82,* 12 January 2007.

99 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

businesses and collectors of tenancy information such as real estate agents.[100] The Australian Communications and Media Authority (ACMA) submitted that:

> The increasing use of technology by small businesses, who may not be experienced in dealing with privacy matters places increasing pressure on the relevance of the small business exemption currently in the Privacy Act.[101]

35.48 Stakeholders also were concerned that consumers may not be able to determine with any certainty whether the small business exemption applies to the business they are dealing with,[102] since annual turnover figures are rarely publicly disclosed.[103] Furthermore, a concern was expressed that businesses themselves may be uncertain as to whether they are covered by the small business exemption—a problem that is further complicated by the conditions that qualify the application of the exemption.[104] For example, the Legal Aid Commission of New South Wales submitted that the Law Council of Australia was unable to provide clear guidance as to whether law firms are covered by the exemption.[105]

35.49 Abacus submitted that the small business exemption means that 'privacy protection is uneven, which adds complexity and confusion to the regime'.[106] The Queensland Government Department of Justice and Attorney-General expressed particular concern about the complexity of the exemptions regime in the educational sector:

> Non-State schools may or may not be required to comply based on a number of tests, for example annual turnover and the collection of 'health information'. Exempt non-state schools may also choose to 'opt in' to the regime. The three tiered approach that currently operates—determined by the size of the school and the collection of one type of information—can create inconsistencies in the management of personal information in educational contexts.[107]

35.50 Concerns have also been raised that the small business exemption, together with the exemption in relation to related bodies corporate, may be used by large

---

100 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.
101 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.
102 Government of South Australia, *Submission PR 187,* 12 February 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
103 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
104 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
105 Ibid.
106 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.
107 Queensland Government, *Submission PR 242,* 15 March 2007.

organisations to evade their responsibility under the *Privacy Act* by transferring data collection activities to a smaller entity within their corporate structure.[108]

35.51 The Government of South Australia submitted that 'business efficacy is not likely to be enhanced by misuse or careless management of personal information'. It considered that the benefits of removing the exemption would include: enhancing the protection of personal information; clarifying consumers' confusion and closing off loopholes under the exemption, thus promoting public confidence in the effectiveness of the privacy regime; creating a level playing field for all small businesses, as currently some small businesses are not exempt and others choose to opt in; promoting good business management practice and helping to build business reputation; and further harmonising the trans-Tasman privacy protection regime.[109]

35.52 The Australian Privacy Foundation took the view that:

> The sensible response is to have a default position of all businesses being subject to the privacy principles, but with an overall reasonable steps qualification applying to all principles. This would allow the Privacy Commissioner to issue guidance about the circumstances in which no steps, or only limited steps, would be reasonable.[110]

Definition of 'small business'

35.53 There are no recent official data showing the number of small business operators in Australia with an annual turnover of $3 million or less. According to the Australian Bureau of Statistics (ABS), however, as at June 2006, there were 1,837,503 small businesses with a turnover of less than $2 million, representing 93.6% of all actively trading businesses in Australia.[111] Therefore, the number of small businesses with an annual turnover of $3 million or less would be over 1.8 million. This figure, however, does not take into account the fact that some small businesses would not qualify for the small business exemption, for example, because they trade in personal information without the consent of the individuals concerned.

35.54 In evidence before the 2000 House of Representatives Committee inquiry, the Department of Employment, Workplace Relations and Small Business stated that:

> given the likelihood of the existence of high privacy risk low staff number businesses in, for example, the personal service sector or the online world, it was decided that an annual turnover figure that would capture the same number of businesses as the ABS measure should be used. The original figure of $1 million would have exempted 986,000 businesses. This equates to 93.8% of the businesses that would be defined as small businesses under the ABS definition. The $3 million threshold exempts 1,040,000 businesses. This equates to 98.9% of small businesses as defined by the

---

108 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

109 Government of South Australia, *Submission PR 187,* 12 February 2007.

110 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

111 Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 6.

> ABS. It was decided by the Government, therefore, that the $3 million turnover threshold best represented a consistent measure of what was a small business. [112]

35.55 The Department also advised the inquiry that:

> based on the ABS *Business Growth and Performance Survey 1997–98*, approximately 94% of all Australian businesses fall under the $3 million threshold. The Department also noted that the survey indicated that the 95% of Australian businesses that are small businesses accounted for only 30% of total sales of goods and services. On this basis the Department estimated that the proportion of private sector business activity undertaken by small businesses was around 30%.[113]

35.56 The 2000 House of Representatives Committee inquiry accepted that any form of threshold would appear arbitrary.[114] It preferred, however, the use of an annual turnover threshold on the basis that the use of employee numbers to define small businesses could have the unintended consequence of exempting high risk internet-based businesses.[115]

35.57 In the context of defining small businesses for the purposes of tax legislation, it has been argued that turnover is preferable to number of employees because turnover is: reasonably well known and understood (although not consistently defined), as it is the most commonly used test in Australia and overseas; and less open to manipulation than measures based on income or taxable income. In addition, it was contended that using employees as a measure of the size of operations could lead to some businesses being classified as small businesses when they should not be due to the increasing use of contractors, and that grouping contractors with employees to determine size would require complicated provisions to distinguish employee-like contractors from truly independent suppliers.[116]

35.58 Submissions to previous inquiries have consistently questioned the rationale for defining small business as businesses with an annual turnover of $3 million or less.[117]

---

112 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.19] (footnotes omitted).

113 Ibid, [2.20] (footnotes omitted). The Australian Bureau of Statistics, *Business Growth and Performance Survey, Financial Year 1997/1998* (1999) was conducted by the ABS from 1994–95 to 1997–98. It has been discontinued since then.

114 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.22].

115 Ibid, [2.21].

116 N Warren, G Payne and H Hodgson, *Research and Recommendations on Definition of Small Business* (2006) Institute of Chartered Accountants in Australia, 22, 23.

117 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.11]; Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.2]–[3.3]; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 182;

Other legislation defines small businesses differently. For example, under the uniform defamation laws, a corporation has no cause of action for defamation concerning the publication of defamatory matter about the corporation unless it is an 'excluded corporation', including one that employs less than 10 employees at the time of the publication.[118] The stated purpose of this provision is to prohibit corporations from suing for defamation unless they are small businesses or non-profit organisations.[119] In New South Wales, anti-discrimination legislation does not apply to employers who employ five or fewer persons in certain circumstances.[120] For the purposes of the goods and services tax, small businesses are those with an annual turnover of $2 million or less.[121]

35.59 The ABS defines small business as 'a business employing less than 20 people'.[122] As at June 2006, there were 1,877,895 businesses that employed less than 20 employees, representing 95.6% of all actively trading businesses in Australia.[123]

35.60 The OPC Review recommended the use of the ABS definition, on the basis that a business' annual turnover is not generally known and that the number of employees may more easily be understood by consumers and other parties. It also considered that, if the definition were expressed in terms of the definitions used by the ABS, the need to amend the *Privacy Act* each time the ABS definition is changed would be avoided.[124]

35.61 The Australian Government did not agree with the definition recommended by the OPC Review, on the basis that:

> redefining the small business exemption in this way could capture some small operators currently not required to comply with the Act and would increase their

---

Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.51]–[4.52].

118 A corporation is an excluded corporation if: (a) the objects for which it is formed do not include obtaining financial gain for its members or corporations; or (b) it employs fewer than 10 persons and is not related to another corporation; and the corporation is not a public body: *Defamation Act 2005* (NSW) s 9(2); *Defamation Act 2005* (Vic) s 9(2); *Defamation Act 2005* (Qld) s 9(2); *Defamation Act 2005* (WA) s 9(2); *Defamation Act 2005* (SA) s 9(2); *Defamation Act 2005* (Tas) s 9(2); *Civil Law (Wrongs) Act 2002* (ACT) s 121(2); *Defamation Act 2006* (NT) s 9(2).

119 See, eg, New South Wales, *Parliamentary Debates*, Legislative Assembly, 13 September 2005, 17635 (B Debus—Attorney General).

120 *Anti-Discrimination Act 1977* (NSW) ss 25(3)(b), 38C(3)(b), 40(3)(b), 49D(3)(b), 49V(3)(b), 49ZH(3)(b).

121 *A New Tax System (Goods and Services Tax) Act 1999* (Cth) ss 131–5, 162–5. Small businesses with an annual turnover that does not exceed $2 million can apportion their input tax credits for acquisitions and importations of goods and services used for non-business purpose that are partly creditable on an annual basis, rather than on a monthly or quarterly basis.

122 D Trewin, *Small Business in Australia—2001* (2002) Australian Bureau of Statistics.

123 Australian Bureau of Statistics, *Counts of Australian Businesses*, 8165.0 (2007), 5.

124 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 184, rec 51.

> costs. It is also inconsistent with cutting regulatory 'red tape' and with workplace reform.[125]

Submissions and consultations

35.62 Many stakeholders identified the definition of 'small business' as problematic. In submissions and consultations, there is recognition—by both proponents and opponents of the small business exemption—that the threshold for the small business exemption of an annual turnover of $3 million or less is arbitrary.[126]

35.63 The Australian Privacy Foundation stated that:

> The small business exemption threshold is completely arbitrary. It is impossible to envisage any sensible size or other criteria which would capture potentially significant personal information handling while excluding 'mundane' processing. Even one-person businesses can be at the forefront of privacy intrusion (e.g. private investigators, or specialised websites).[127]

35.64 The OPC reiterated its recommendation in the OPC Review that the definition of small business be expressed in terms of the ABS definition of small business.[128]

35.65 There was some opposition to the OPC's recommendation.[129] The ACCI did not consider it appropriate to define small business in terms of the number of employees, on the basis that:

> - as casual or part time employees are counted as a single employee, this test would capture many small businesses who are currently exempt under the $3 million threshold test, particularly service industries, which are heavily reliant on casual labour; and
> - it would vastly increase costs of such small businesses.[130]

35.66 Electronic Frontiers Australia opposed an exemption based on the number of employees because 'this would still result in exemption for organisations that collect and disclose substantial amounts and types of personal information'.[131] Like the

---

125 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 10.

126 Council of Small Business Organisations of Australia Ltd, *Submission PR 203,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

127 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

128 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

129 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

130 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

131 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

Australian Privacy Foundation, Electronic Frontiers Australia took the view that even a sole trader may handle large amount of personal information.[132]

High risk sectors

35.67 Submissions to the OPC Review and the 2005 Senate Committee privacy inquiry suggested that some small businesses have significant holdings of personal information and carry out some of the most privacy intrusive activities. These include: tenancy database operators; telecommunication businesses, such as internet service providers (ISPs); debt collectors; private detectives; and dating agencies.[133]

Residential tenancy databases

35.68 Tenancy databases are privately owned electronic databases that contain information on tenants to assist property managers and landlords in assessing risk and identifying potential problem tenants. The *Privacy Act* generally applies to tenancy databases regardless of whether they are run by small businesses, because they trade in personal information. If a tenancy database that is a small business obtains the consent of an individual for the collection or disclosure of his or her personal information, however, then the Act does not apply.[134]

35.69 The 2000 House of Representatives Committee inquiry recommended that the NPPs apply to tenancy databases and that the Australian Government ensure that tenancy databases do not gain the benefit of the small business exemption.[135] This recommendation was rejected by the Attorney-General's Department because it did not believe that there was 'sufficient justification for singling out tenancy databases from the small business exemption'.[136]

35.70 The OPC Review recommended that the Attorney-General consider regulations to ensure that the *Privacy Act* applies to all small businesses operating residential tenancy databases.[137] It also recommended that the Privacy Commissioner be empowered to make a binding code under the Act to apply to all residential tenancy databases.[138] The 2005 Senate Committee privacy inquiry expressed concern that regulating small businesses in some areas—such as tenancy databases and

---

132 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

133 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 180; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.48]–[4.49].

134 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 72.

135 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), rec 19.

136 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

137 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 9, 15, 52.

138 Ibid, rec 16.

telecommunications—but not others would only add to the complexity of the legislation.[139]

35.71 In 2006, the joint working party established by the Ministerial Council on Consumer Affairs and the Standing Committee of Attorneys-General released a report on residential tenancy databases. The joint working party recommended that the *Privacy Act* apply to residential tenancy databases. Like the OPC Review, the joint working party recommended that regulations be made to prescribe residential tenancy databases as organisations for the purposes of the Act. It also recommended that the Australian Government consider the recommendation in the OPC Review that a binding code be made under the *Privacy Act* to apply to all residential tenancy databases.[140] In addition, the joint working party recommended that 'the states and territories develop agreed uniform model legislation on the use by landlords, agents and listing parties of [residential tenancy databases]'.[141]

35.72 On 30 October 2006, in response to the joint working party's recommendations, the Attorney-General announced that regulations would be made pursuant to s 6E of the *Privacy Act* to prescribe all residential tenancy database operators as 'organisations' under the Act.[142]

35.73 The relevant state and territory ministers also have agreed to adopt uniform model residential tenancy database legislation. The Queensland Government will be drafting the model legislation.[143] Issues concerning residential tenancy databases are discussed further in Chapter 14.

Telecommunications industry

35.74 Although the use and disclosure of information by telecommunication providers with an annual turnover of $3 million or less are regulated by Part 13 of the *Telecommunications Act 1997* (Cth), they are not required to observe any standards when engaging in other information-handling practices—such as the collection and storage of personal information—if they have the consent of the individuals concerned when trading in the individuals' personal information.[144]

---

139 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32].

140 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), 49–50.

141 Ibid, 48, 50.

142 P Ruddock (Attorney-General), 'More Protection for Tenants' Privacy' (Press Release, 30 October 2006).

143 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 3.

144 The privacy issues concerning telecommunications service providers are discussed in detail in Part J.

35.75 The OPC Review recommended that the Attorney-General consider regulations to ensure that the *Privacy Act* applies to all small businesses in the telecommunications sector.[145] The 2005 Senate Committee privacy inquiry expressed concern that regulating small businesses in some areas—such as tenancy databases and telecommunications—but not others would only add to the complexity of the legislation.[146]

35.76 In its response to the OPC Review, the Australian Government stated that the Attorney-General's Department would, in conjunction with the relevant government agencies, consider making regulations to ensure that the *Privacy Act* applies to all small businesses in the telecommunications sector.[147]

Debt collectors

35.77 The *Privacy Act* does not generally apply to debt collectors that have an annual turnover of $3 million or less. A debt collection agency that has purchased debts from a credit provider, however, may qualify as a credit provider and be subject to the credit reporting provisions of the Act. In addition, they are regulated by the consumer protection provisions of the *Trade Practices Act 1974* (Cth), the *Australian Securities and Investments Commission Act 2001* (Cth) and other relevant state legislation.[148] Issues concerning the application of the credit reporting provisions of the Act to debt collectors are discussed in Chapter 53.

Small businesses that hold genetic information

35.78 In their report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council noted that there was some doubt as to whether all small businesses that hold genetic information are subject to the *Privacy Act*.[149] It was considered that acts and practices of small businesses that hold genetic information pose a potential risk to the privacy of both the individual and

---

145 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 9, 15, 52.

146 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32].

147 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 3.

148 The Australian Competition and Consumer Commission and the Australian Securities and Investments Commission, who are jointly responsible for enforcing consumer protection legislation in relation to the debt collection industry, have issued guidance to assist collectors and creditors in understanding how the legislation applies to them: Australian Competition and Consumer Commission and Australian Securities and Investment Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

149 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.104]. Submissions to ALRC 96 suggested that small businesses may not be covered by the *Privacy Act* if they simply store genetic samples or act as a data repository, without providing a health service; or if they are genomics companies that undertake research and do not trade in personal information: Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.100]–[7.101].

his or her genetic relatives.[150] The ALRC and AHEC recommended in ALRC 96 that the *Privacy Act* be amended to ensure that all small businesses that hold genetic information are subject to the provisions of the Act, regardless of whether they provide a health service.[151]

35.79 The *Privacy Legislation Amendment Act 2006* (Cth) has amended the definitions of 'health information' and 'sensitive information' in the *Privacy Act* to include genetic information about an individual.[152] This means that small businesses that hold genetic information and provide a health service do not fall under the small business exemption.

Submissions and consultations

35.80 Submissions confirmed that there are significant concerns that certain sectors pose a particularly high risk to privacy and therefore should not be exempt from the *Privacy Act*.[153]

35.81 The Consumer Credit Legal Centre (NSW) (CCLC) submitted that:

> some of the most intrusive activities are carried out by very small organisations, and even sole traders, for example, private detectives, debt collectors, internet service providers and dating agencies.
>
> In several key areas we consider that the benefits of the small business exemption do not outweigh the disadvantages for business and for individuals. The key areas are industries that control large amounts of personal information and that also have access to the credit reporting system. Two particular industries are telecommunications and finance. Notably both industries were traditionally dominated by large companies that would not be classified as small businesses for the purposes of the Act. This is no longer the case and there are now many businesses in both finance and telecommunications that would fall under the small business exemption.[154]

35.82 Consistent with its recommendation in the OPC Review, the OPC submitted that some small business sectors that handle significant amounts of personal information should be prescribed as 'organisations' under the *Privacy Act*. It considered that coverage of the *Privacy Act* should be extended to: all small businesses in the telecommunications sector, including ISPs and Public Number Directory Producers;

---

150 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.102].

151 Ibid, Rec 7–7.

152 *Privacy Legislation Amendment Act 2006* (Cth) sch 2 cl 2. The Australian Democrats unsuccessfully sought to remove the small business exemption, the political party exemption and the exemption for political acts and practices during parliamentary debate on the legislation: Commonwealth, *Parliamentary Debates*, Senate, 7 September 2006, 42 (N Stott Despoja).

153 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

154 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

small businesses that collect and use biometric information; and estate agents, landlords and listing agents who use residential tenancy databases.[155]

Residential tenancy database

35.83 The OPC noted that in addition to small businesses that operate residential tenancy databases, other users of the databases could also fall under the small business exemption—for example, estate agents that conduct database reporting on residential tenants, particularly if the agents have the consent of the individual concerned. The OPC further suggested that:

> if the states and territories do not pass uniform legislation to regulate estate agents, landlords and listing agents who use Residential Tenancy Databases (RTDs), that these businesses should be prescribed as organisations under the Act.[156]

35.84 The REIA supported the introduction of regulations pursuant to s 6E of the *Privacy Act* to prescribe all residential tenancy databases as 'organisations' for the purposes of the *Privacy Act*.[157]

Telecommunications industry

35.85 Some stakeholders, including the Department of Communications, Information Technology and the Arts (DCITA) and ACMA, expressed particular concern that small business operators in the telecommunications industry are exempt from the *Privacy Act*.[158]

35.86 DCITA did not consider it appropriate to treat small businesses in the telecommunications industry differently from medium and large businesses:

> As [the small business exemption] would effectively exempt a broad section of the telecommunications sector, we do not consider it appropriate to treat small businesses in the telecommunications industry differently from medium and large businesses. This is particularly the case in relation to the protection of the contents and substance of communications and the use and disclosure of personal information contained in the [Integrated Public Number Database].[159]

35.87 ACMA noted that more than a quarter of ISPs are small business operators. It expressed concern that carriage service providers, including ISPs, that are small businesses are exempt from the *Privacy Act* and questioned the relevance of the small business exemption in the increasingly convergent telecommunications environment.

---

155 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
156 Ibid.
157 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.
158 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007; Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
159 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

> Most consumers have little or no knowledge of the exemptions to the Privacy Act. As a consequence, many consumers transact with businesses assuming that their personal information is protected by the Privacy Act, when this may not be the case. If the small business exemption is to continue, it may be beneficial to publicise the exemption. This activity may result in voluntary compliance becoming a key market differentiator.[160]

35.88 Electronic Frontiers Australia submitted that all small businesses involved in the telecommunications and internet services sector should be required to comply with the NPPs, on the basis that the *Telecommunications Act* does not cover the collection of personal information.[161]

35.89 By contrast, the Communications Alliance submitted that:

> Whilst we concede that there are non-complying operators in the telecommunications sector that fall within the small business exemption, Communications Alliance recommends education and awareness raising and incentives to industry for voluntary adoption of the NPPs as a way to resolve the problem, rather than additional codes which will only increase the regulatory burden on small business operations.[162]

Debt collection

35.90 The CCLC submitted that a small business exemption should not apply in relation to debt collection, because when a bank sells the debt to a debt collector who is covered by the small business exemption, 'the strict confidentiality the consumer expected when entering into the loan has now been eroded often without their knowledge'. It contended that 'a consumer should be able to expect that the privacy rights that consumer had upon entering the loan are preserved for the life of the debt'.[163]

35.91 On the other hand, Abacus, while acknowledging that debt collection activity may fall under the small business exemption even though the debtor borrowed from a larger financial institution, suggested that:

> The 2005 renewal of the ASIC/ACCC Debt Collection Guidelines does, in *Abacus's* view, provide some confidence that creditors will ensure any debt recovery action is undertaken in accord with privacy measures.[164]

---

160 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

161 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007, referring to Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999).

162 Communications Alliance Ltd, *Submission PR 198,* 16 February 2007.

163 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

164 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007, referring to Australian Competition and Consumer Commission and Australian Securities and Investment Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

Other industries or services

35.92 Some stakeholders also have suggested other high risk sectors to which the small business exemption should not apply.[165] The NSW Commissioner for Children and Young People expressed concern that services such as child care centres, family counselling or dispute resolution services—which often keep records of sensitive personal information of children and young people—may fall within the small business exemption. It submitted that the *Privacy Act* should be amended to include specifically any business that provides services to children and young people.[166]

35.93 Another stakeholder expressed concern about the retention and use of personal records by the recruitment industry, in circumstances where jobseekers would have to consent to disclosure of their personal information in order to obtain the recruitment organisation's services.[167]

35.94 AXA submitted that 'it is not appropriate to exempt the financial services sector from the *Privacy Act*'.[168]

Modifying the application of the privacy principles to small businesses

35.95 A few stakeholders submitted that there are other ways to minimise the compliance burden on small businesses without the need for an exemption. It was suggested that this could be achieved by modifying the application of the privacy principles to small businesses, through:

- a privacy code for small businesses, which would relax or remove bureaucratic aspects of the principles and the *Privacy Act* while ensuring that personal information is handled appropriately;[169]
- public interest determinations issued by the Privacy Commissioner; or [170]
- specific exceptions to the privacy principles in relation to small businesses.[171]

---

165 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007; AXA, *Submission PR 119,* 15 January 2007; Confidential, *Submission PR 97,* 15 January 2007.

166 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

167 Confidential, *Submission PR 97,* 15 January 2007. Although recruitment organisations trade in personal information, under s 6D(7)(a) of the *Privacy Act*, a recruitment organisation that has an annual turnover of $3 million or less may still be covered by the small business exemption if it has the consent of the individuals concerned. It also should be noted that the acts and practices of a recruitment organisation do not fall within the employee records exemption, unless they are in relation to the employee records of a current or former employee of that recruitment organisation and are directly related to that current or former employment relationship: see Information Technology Contract & Recruitment Association, *Privacy and the Recruitment Industry* <www.itcra.com/index.asp?menuid=100.010&artid=119> at 1 August 2007. The employee records exemption is discussed in Ch 36.

168 AXA, *Submission PR 119,* 15 January 2007.

169 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

170 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

171 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

EU adequacy and implementation of the APEC Privacy Framework

35.96 A further argument for the removal of the small business exemption is that its existence is one of the major obstacles to Australia's privacy law being recognised as adequate by the EU, thus, arguably, impeding trade with the EU. One of the objectives of the private sector provisions of the *Privacy Act* was to facilitate trade with the EU.[172]

35.97 In March 2001, the Article 29 Data Protection Working Party of the European Commission released an opinion expressing concern about the sectors and activities excluded from the protection of the *Privacy Act*. The small business and employee records exemptions were noted as particular areas of concern.[173]

35.98 As the EU Directive restricts the export of personal data from an EU Member State to a recipient country that does not have an 'adequate level of protection',[174] Australian businesses that wish to trade with EU organisations would need to have contractual clauses in place to ensure the adequate protection of personal data transferred from the EU.[175]

35.99 The OPC Review noted that negotiations with the European Commission on this issue were continuing, especially in relation to the small business and employee records exemptions.[176] The Review concluded that, although there was no evidence of a broad business push for EU adequacy, there may be long term benefits for Australia in achieving such adequacy. The OPC Review therefore recommended that the Australian Government continue to work with the EU on this issue.[177] The Australian Government agreed with this recommendation.[178]

35.100 In addition, the OPC Review noted that globalisation of information makes implementation of international privacy frameworks important. Therefore the OPC also recommended that the Australian Government continue to work within APEC to implement the APEC Privacy Framework.[179]

---

172 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 16.

173 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 3.

174 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 25, 26.

175 Ibid, art 26(2).

176 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

177 Ibid, rec 17.

178 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 4.

179 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 17.

Submissions and consultations

35.101 A number of stakeholders were of the view that the removal of the small business exemption would assist to ensure that Australia's privacy law is recognised as adequate by the EU.[180] One stakeholder submitted that Australian privacy laws should be consistent with international standards and therefore Australia should aim to achieve EU adequacy.[181] Professor Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that the exemption is a considerable obstacle for any adequacy finding. They noted that an European company would not be able to ascertain whether a business is an exempt small business for the purposes of the *Privacy Act*. They stated that:

> If personal data are transferred from Europe to some proper recipient in Australia, there is nothing in the Privacy Act except the normal rules governing secondary purposes to prevent the data from being disclosed to an exempt small business operator.[182]

35.102 The Australian Bankers' Association (ABA) submitted that the lack of EU adequacy has significant disadvantages for Australian companies that operate in a European environment. 'An Australian company must comply with the EU Directive through the exemptions (conditions) on a case by case basis when transferring data from an EU country to Australia'. The ABA submitted that removal of the small business exemption would remove a significant impediment to a finding of EU adequacy.[183]

35.103 Some stakeholders submitted that, as Australia's privacy laws are not being recognised as adequate by the EU, Australian businesses that wish to trade with organisations in the EU have to bear the costs of additional contractual arrangements,[184] including the costs of periodic audits of compliance with these arrangements.[185]

35.104 In contrast, the REIA suggested that:

> the APEC Privacy Framework is more closely aligned with the interests of Australia, and that Australia should not pursue a declaration of adequacy under the floundering EU Privacy Directive if this comes at the cost of the small business exemption. Small businesses experiencing problems obtaining personal data from European suppliers may always 'opt in' to the Australian privacy regime, which should 'in principle' be recognized by the EU similarly to businesses operating under the US Safe Harbor

---

180 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

181 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

182 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

183 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

184 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

185 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

> Privacy Principles. Further, the Australian Government may mandate that certain otherwise exempt entities be made subject to the Privacy Act 1988.[186]

Voluntary compliance and opting in

35.105 In practice, some small businesses appear to have committed to comply voluntarily with the *Privacy Act* without using the opt-in mechanism—for example, by posting privacy policies on their websites, or by agreeing to contractual terms that require them to comply with the *Privacy Act*. In a number of case studies, it was observed that some small businesses have privacy policies that state that they are bound by the *Privacy Act* even though they have not opted in.[187] It has been argued that, since such small businesses have not opted in, this leaves consumers or the other contracting party with limited avenues of complaint.[188]

35.106 In IP 31, the ALRC asked whether the opt-in procedure should continue to be available.[189] A number of submissions supported the retention of the opt-in procedure.[190] The OPC submitted that the opt-in provision in s 6EA of the *Privacy Act* should be retained because:

> it provides a mechanism for businesses to enhance their business reputation, and in some cases it is a requirement if the organisation wants to apply for a Code or Public Interest Determination.[191]

35.107 The Australian Government Department of Employment and Workplace Relations submitted that the opt-in mechanism represents 'a market solution to the question of which small businesses should monitor and control their handling of personal information':

> there is a role for privacy-savvy customers and other organisations having business dealings with small business to alert small business to privacy concerns, and to use their market power to persuade small business to 'opt in' or otherwise incorporate privacy safeguards in their business practices.[192]

35.108 The ACCI stated that it would not oppose an opt-in mechanism, provided that it remains voluntary. It suggested, however, that given the low uptake of the opt-in

---

186 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

187 M Jackson and others, *Small Business: Issues of Identity Management, Privacy and Security* (2006), 9–10.

188 Ibid, 9–10.

189 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–6.

190 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

191 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

192 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

procedure by small businesses, the procedure be discontinued if the cost is disproportionate to the benefit of opting in.[193]

35.109 On the other hand, the ABA submitted that the opt-in mechanism would not be required if the Privacy Commissioner were to develop a public interest determination modifying the application of the NPPs to small businesses.[194]

ALRC's view

35.110 The ALRC is not convinced that an exemption for small business is either necessary or justifiable. While cost of compliance with the *Privacy Act* is an important consideration, this factor alone does not provide a sufficient policy basis to support the exemption. Further, the fact that no comparable overseas jurisdictions—including the United Kingdom, Canada and New Zealand—have an exemption for small businesses is a relevant consideration.

35.111 At present, subject to some businesses not meeting the conditions that qualify the application of the small business exemption, potentially up to 94% of businesses are exempt from the *Privacy Act*. The ALRC considers that the risks to privacy posed by small businesses are determined by the amount and nature of personal information held, the nature of the business and the way personal information is handled by the business, rather than by their size alone. Some small businesses, such as internet service providers and debt collectors, hold large amounts of personal information. In addition, given the increasing use of technology by small businesses, the risk posed to privacy may not necessarily be low. In this regard, it should be noted that the OPC received a significant number of inquiries that related to this exemption.

35.112 The ALRC does not consider that modifying the exemption is a sufficient response to the concerns raised in submissions and consultations. Whatever the threshold for the exemption is, the definition of 'small business' would be arbitrary, and consumers cannot determine easily whether the exemption applies to a particular business. In some cases, even small businesses may have problems understanding whether the exemption applies to them due to the various conditions for the application of the exemption.

35.113 The ALRC agrees with the 2005 Senate Committee privacy inquiry that regulating small businesses in some areas—such as residential tenancy databases, telecommunications and debt collection—and not others, would add to the complexity of the privacy regime. Modifying the application of the privacy principles to small businesses, either through a code, a public interest determination by the OPC or specific exceptions to certain privacy principles, would also result in uneven privacy protection without adequately addressing concerns about unnecessary costs of compliance to small businesses.

---

193 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
194 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

35.114 Further, while the ALRC acknowledges that there is no broad push for Australia to achieve 'adequacy status' under the EU Directive, the removal of the exemption may assist in achieving EU adequacy and facilitate trade with EU organisations.

35.115 The ALRC acknowledges that removal of the exemption will result in compliance costs for small businesses. Costs are a legitimate concern for small businesses and for policy makers. There are, however, a number of ways that unnecessary compliance costs can be minimised without compromising individual privacy.

35.116 The costs of compliance are in part due to the complexity of the *Privacy Act*. In Chapter 3, the ALRC proposes that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity, and that the privacy principles be streamlined. The simplification of the legislation should go some way towards reducing unnecessary costs of compliance to small businesses.

35.117 Another way to reduce compliance costs to small businesses is by assisting them in understanding their regulatory rights and obligations.[195] The ALRC considers that this can be achieved by the OPC providing dedicated assistance and support to small businesses, which would include: a special national helpline for small businesses, similar to the Australian Competition and Consumer Commission's small business helpline;[196] developing guidelines and other educational material; providing templates for Privacy Policies free of charge; and liaising with other government departments and industry bodies—such as the Office of Small Business, the Business Council of Australia and the ACCI—to provide educational programs targeted at small businesses.[197] This may eliminate the need for small businesses to obtain legal advice, and may assist in the provision of training for staff in relation to compliance with the *Privacy Act*.

35.118 Such assistance should be established before the proposed removal of the exemption comes into effect. This would ensure that small businesses have sufficient

---

195 Small Business Ministers Council, *Giving Small Business a Voice—Achieving Best Practice Consultation with Small Business (Endorsed Paper)* (2000) Australian Government Office of Small Business.

196 The helpline was established to assist small businesses in complying with the *Trade Practices Act 1974* (Cth): Australian Competition and Consumer Commission, *Easy Access for Small Business for Advice* (2005) <www.accc.gov.au/content/index.phtml/itemId/718924> at 1 August 2007.

197 It should be noted that, currently, the OPC provides a number of plain English resources to assist small businesses in understanding whether they are covered by the *Privacy Act* and, if so, their obligations under the Act, including, eg, Office of the Privacy Commissioner, *A Snapshot of the Privacy Act for Small Business* <www.privacy.gov.au/business/small/bp.html> at 1 August 2007; Office of the Privacy Commissioner, *A Privacy Checklist for Small Business* <www.privacy.gov.au/business/small/index.html> at 1 August 2007; Office of the Privacy Commissioner, *A Guide to Privacy for Small Business* <www.privacy.gov.au/business/small/bizguide.html> at 1 August 2007.

time to understand their obligations under, and prepare for compliance with, the *Privacy Act* once the exemption is removed.

35.119 The ALRC acknowledges that such dedicated assistance to small businesses will have resource implications for the OPC and may require an increase in funding to the OPC by the Australian Government.

Proposal 35–1 The *Privacy Act* should be amended to remove the small business exemption by:

(a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and

(b) repealing ss 6D–6EA of the Act.

Proposal 35–2 Before the proposed removal of the small business exemption from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by:

(a) establishing a national small business hotline to assist small businesses in complying with the Act;

(b) developing educational materials—including guidelines, information sheets, fact sheets and checklists—on the requirements under the Act;

(c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge; and

(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding and acceptance of the privacy principles.

36. Employee Records Exemption

Contents

Introduction 1039
Current law 1039
Adequacy of privacy protection for employee records 1043
Background 1043
EU adequacy and implementation of the APEC Privacy Framework 1045
Submissions and consultations 1046
ALRC's view 1054
Evaluative material 1056
Submissions and consultations 1057
Options for reform 1058
ALRC's view 1060
Location of privacy provisions concerning employee records 1061
Submissions and consultations 1062
ALRC's view 1063

Introduction

36.1 An organisation that is or was an employer of an individual is exempt from compliance with the *Privacy Act 1988* (Cth) where an act or practice is directly related to the employment relationship and to an employee record held by the organisation. This chapter considers whether this exemption should remain.

Current law

36.2 Section 6 of the Act defines 'employee record' to mean a record of personal information relating to the employment of the employee. Examples of such personal information include health information about the employee, and personal information about:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee's personal and emergency contact details;

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

(h) the employee's membership of a professional or trade association;

(i) the employee's trade union membership;

(j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;

(k) the employee's taxation, banking or superannuation affairs.[1]

36.3 Acts and practices of an organisation are exempt from the *Privacy Act* if they are directly related to a current or former employment relationship.[2] Accordingly, the exemption does not apply to: acts and practices of an employer that are beyond the scope of the employment relationship;[3] the personal information of unsuccessful job applicants;[4] and the handling of employee records by contractors and subcontractors to the employer.[5]

36.4 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) stated that:

> The act or practice must be directly related to a current or former employer relationship so as to ensure that employers cannot use 'employee records' for commercial purposes unrelated to the employment context.[6]

36.5 The reason given for the employee records exemption was that:

> While this type of personal information is deserving of privacy protection, it is the government's view that such protection is more properly a matter for workplace relations legislation.[7]

---

1 *Privacy Act 1988* (Cth) s 6(1). This list is not intended to be exhaustive: Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [22]. Some information held by employers relating to individual employees—for example, emails received by an employee from third parties—may not necessarily be an 'employee record': Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 3.

2 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(3).

3 For example, employers cannot sell a list of employees for marketing purposes: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 3. See also *C v Commonwealth Agency* [2005] PrivCmrA 3, in which the Privacy Commissioner determined that the disclosure of an employee record by an employer to the employer's legal counsel in relation to proceedings that did not concern the employee was not an act that was directly related to the employment relationship, and therefore did not fall within the employee records exemption.

4 Once an employment relationship is established, however, records of pre-employment checks on the individual employee become exempt: Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 3.

5 Ibid, 4. The Office of the Privacy Commissioner has stated that 'in many circumstances, the exemptions may not apply to organisations that provide recruitment, human resource management services, medical, training or superannuation services under contract to an employer': Office of the Federal Privacy Commissioner, *Coverage of and Exemptions from the Private Sector Provisions (Updated with Minor Amendments 6/9/02)*, Information Sheet 12 (2001), 3.

6 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [109].

36.6 The website of the Australian Government Attorney-General's Department (AGD) indicates that:

> The potential also exists for Commonwealth privacy regulation of employee records to have unintended consequences where it intersects with State and Territory laws dealing with employee records.[8]

36.7 Currently, there is little privacy protection for private sector employees under the federal workplace relations regime. Regulations 19.20 and 19.21 of the *Workplace Relations Regulations 1996* (Cth) allow employees to access certain records. This, however, only applies to records about conditions under which employees are hired, hours worked, remuneration, leave, superannuation contributions and termination.[9] It does not include other personal information that falls within the definition of 'employee record' in the *Privacy Act*, for example, employees' health information, or their taxation or banking affairs. The regulations only require employers to maintain and provide access to records, rather than to protect the privacy of those records.

36.8 There is no corresponding exemption for the handling of employee records by agencies under the *Privacy Act*. Therefore, Australian Government and ACT agencies are required to comply with the Information Privacy Principles (IPPs) when dealing with employee records.[10] Privacy legislation in New South Wales, Victoria and the Northern Territory also applies to employee records of public sector employees.[11] In Tasmania, public sector bodies, councils, the University of Tasmania, prescribed bodies, and contractors to these entities have to comply with the personal information protection principles under the *Personal Information Protection Act 2004* (Tas) in dealing with employee information, subject to certain exceptions.[12] The Victorian *Health Records Act 2001* also regulates the handling of health information, including information contained in employee records, by public and private sector entities.

36.9 A number of overseas jurisdictions—including the United Kingdom, Ireland, New Zealand and Hong Kong—do not exempt employee records from the operation of their privacy or data protection legislation. They do, however, commonly provide for exceptions to their data protection principles when dealing with personal information

---

7 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15752. See also Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, notes on clauses [109].

8 Australian Government Attorney-General's Department, *Employee Records* (2000) <www.ag.gov.au> at 14 August 2007.

9 *Workplace Relations Regulations 2006* (Cth) regs 19.7–19.16.

10 A slightly amended version of the *Privacy Act 1988* (Cth) applies to ACT government agencies: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) s 23.

11 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic); *Information Act 2002* (NT).

12 *Personal Information Protection Act 2004* (Tas) ss 3 (definition of 'personal information custodian'), 10, sch 1, cl 2(1)(i)–(j).

for the purposes of recruitment, appointments and contracts for provision of services.[13] Some overseas legislation also provides an exception for personal references relevant to an individual's suitability for employment or appointment to office.[14]

36.10 There is no general exemption for employee records under the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines), the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[15]

36.11 In 2001, the Article 29 Data Protection Working Party of the European Commission released its advisory opinion on the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Working Party stated that employee records often contain sensitive information and saw no reason to exclude them from the protection provided for sensitive information by National Privacy Principle (NPP) 10. Furthermore, the Working Party observed that the exemption allows information about previous employees to be collected and disclosed to a third party (eg, a future employer) without the employee being informed.[16]

36.12 For the period from 21 December 2001 to 31 January 2005, the Office of the Privacy Commissioner (OPC) indicated that 12% of all the NPP complaints closed by the Office as outside of its jurisdiction concerned the employee records exemption.[17] In 2005–06, the OPC received 2,000 enquiries concerning exemptions, of which 43% related to the employee records exemption.[18]

---

13 See, eg, *Data Protection Act 1998* (UK) sch 7, cls 3, 4; *Data Protection Act 1988* (Ireland) s 4(13); *Personal Data (Privacy) Ordinance* (Hong Kong) s 55.

14 See, eg, *Data Protection Act 1998* (UK) sch 7, cl 1; *Privacy Act 1993* (NZ) s 29(1)(b); *Personal Data (Privacy) Ordinance* (Hong Kong) s 56.

15 Article 8(2)(b) of the EU Directive, however, provides that processing of certain sensitive personal data may be allowed if it is 'necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards': European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 8(2)(b). The APEC Privacy Framework provides that when using personal information for employment purposes, employers may not need to comply with the principle that individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information in certain situations: Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [20].

16 European Union Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 Final (2001), 4. One commentator suggests that this misstates the position in that the exemption does not allow a past employer to forward information to a prospective employer without informing the employee: P Ford, 'Implementing the EC Directive on Data Protection—An Outside Perspective' (2003) 9 *Privacy Law & Policy Reporter* 141, 145.

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

18 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 27.

Adequacy of privacy protection for employee records

Background

36.13 In 2000, the House of Representatives Standing Committee on Legal and Constitutional Affairs concluded an inquiry into the Privacy Amendment (Private Sector) Bill (2000 House of Representatives Committee inquiry). The 2000 House of Representatives Committee inquiry was not satisfied that existing workplace relations legislation provided adequate protection for the privacy of private sector employee records, and expressed 'grave concerns' about the exemption.[19]

36.14 The 2000 House of Representatives Committee inquiry stated that employees are in need of privacy protection because employers frequently hold a large amount of information about their employees, some of which can be extremely sensitive—such as health information, genetic test results, financial details and results of psychological testing conducted before employment. The inquiry acknowledged that there are competing considerations and that employers should be able to disclose some information to future employers, such as confidential references. It considered that a distinction could be drawn in the nature, but not the sensitivity, of the information that may be held in employee records. It was the inquiry's view that employees are entitled to expect confidentiality of their workplace records given that they have little choice about providing information to their employers.[20]

36.15 A particular issue was whether the health information of employees should be covered by the *Privacy Act*. The 2000 House of Representatives Committee inquiry strongly objected to the inclusion of 'health information' in the definition of 'employee record'. It also noted that this was inconsistent with the more specific protection given to health information and sensitive information elsewhere in the Privacy Amendment (Private Sector) Bill.[21]

36.16 In rejecting the recommendations by the 2000 House of Representatives Committee inquiry, the Australian Government stated that:

> The regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The Government considers that to attempt to deal with employee records in the [Privacy Amendment

19 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.29].
20 Ibid, [3.30]–[3.33].
21 Ibid, [3.37].

> (Private Sector)] Bill might result in an unacceptable level of interference with those State and Territory laws, and a confusing mosaic of obligations.[22]

36.17 In their 2003 report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council recommended that the *Privacy Act* be extended to cover genetic information contained in employee records.[23] The ALRC and AHEC further recommended that the forthcoming inter-departmental review of employee privacy by the AGD and the Australian Government Department of Employment and Workplace Relations (DEWR) consider whether the *Privacy Act* should be amended to cover other forms of health information contained in employee records.[24]

36.18 In February 2004, the AGD and DEWR released a discussion paper on the privacy of employee records.[25] The discussion paper examined the current level of privacy protection for employee records under existing federal, state and territory laws. It also considered some privacy concerns about employee records and suggested options for enhancing privacy. These options included: retaining the exemption; abolishing or modifying the exemption; establishing specific employee records privacy principles; and protecting employee records in workplace relations legislation.[26] No final recommendations were made.

36.19 In its report, *Workplace Privacy—Final Report* (2005), the Victorian Law Reform Commission (VLRC) commented that 'the operation of the employee records exemption leaves a significant gap in the privacy protection of workers' personal information'.[27]

36.20 In April 2006, the Standing Committee of Attorneys-General agreed to establish a working group to advise ministers on options for improving consistency in privacy

---

22 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007. During the OPC Review, a number of submissions and consultations commented on the employee records exemption, despite the fact that it was expressly excluded from the terms of reference for the Review: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 285.

23 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 34–1.

24 Ibid, Rec 34–2.

25 Australian Government Attorney-General's Department and Australian Government Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (2004).

26 Ibid, [4.15]–[4.42]. The 2005 Senate Committee privacy inquiry expressed disappointment at the slow progress of the AGD and DEWR review, and considered the finalisation and release of the results of the review a matter of urgency: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.35].

27 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [1.19].

regulation, including workplace privacy.[28] In its response to the 2006 report by the Productivity Commission's Taskforce on Reducing Regulatory Burdens on Business, the Australian Government stated that the working group would liaise with—and not duplicate the work of—the ALRC in this area.[29]

36.21 In November 2006, the House of Representatives Standing Committee on Legal and Constitutional Affairs released a report on the harmonisation of legal systems within Australia and between Australia and New Zealand. In its report, the Committee recommended that 'the Australian Government highlight the issue of regulatory inconsistency in privacy regulation, including in the area of workplace privacy regulation', in its submissions to the current Inquiry.[30]

EU adequacy and implementation of the APEC Privacy Framework

36.22 The European Union (EU) has not granted Australia 'adequacy status' under the EU Directive.[31] The OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) noted that there were continuing negotiations with the European Commission regarding the adequacy of the *Privacy Act*, especially in relation to the small business and employee records exemptions.[32] The OPC Review concluded that, although there was 'no evidence of a broad business push' for achieving EU adequacy, there may be long term benefits for Australia in achieving such adequacy. The OPC Review therefore recommended that the Australian Government continue to work with the EU on this issue.[33] The Australian Government agreed with this recommendation.[34]

36.23 In addition, the OPC Review noted that the increase in transborder data flows makes implementation of international privacy frameworks important. The OPC therefore also recommended that the Australian Government continue to work within APEC to implement the APEC Privacy Framework.[35]

---

28 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), 26.

29 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

30 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Harmonisation of Legal Systems within Australia and between Australia and New Zealand* (2006), rec 25.

31 See European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 14(b).

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

33 Ibid, rec 17.

34 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 4.

35 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 17.

36.24 In its inquiry into the *Privacy Act* in 2005, the Senate Legal and Constitutional References Committee (2005 Senate Committee privacy inquiry) noted with concern that current workplace relations legislation does not adequately protect workplace privacy, and recommended that this Inquiry examine the precise mechanisms under the *Privacy Act* to protect employee records.[36] It also recommended that the current Inquiry investigate possible measures that could assist Australia in achieving EU adequacy.[37] The Australian Government disagreed with this recommendation, on the basis that 'international negotiations are a matter for the Australian Government and negotiations with the European Union are ongoing'.[38] The issue of EU adequacy is discussed further in Chapter 28.

Submissions and consultations

36.25 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the employee records exemption should remain.[39] A large number of stakeholders supported the removal of the employee records exemption.[40]

36.26 Some stakeholders observed that employers sometimes hold sensitive personal information about their employees, such as health, financial or disabilities information.[41] The Centre for Law and Genetics suggested that there is a real potential for individuals to be harmed if such sensitive personal information is inappropriately used or disclosed.[42] The Queensland Council for Civil Liberties submitted that 'employees usually have no effective choice but to give significant personal information, often of a sensitive nature to their employer'.[43] Similarly, the ACTU stated:

---

36 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.36]–[7.38]; recs 13, 14.

37 Ibid, rec 16.

38 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006), 5.

39 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–9.

40 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; ACTU, *Submission PR 155,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

41 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; ACTU, *Submission PR 155,* 31 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

42 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

43 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007, quoting Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.17].

> In many cases information is collected from employees as a condition of their employment; for example, health information, criminal charges or convictions and financial matters such as bankruptcy or garnishee of wages. The exemption allows this information to be disclosed to others in circumstances which could be very damaging to the individual.[44]

36.27 Stakeholders raised particular concerns about the privacy of employees' health information.[45] For example, the Victorian Office of the Health Services Commissioner stated that it has received many inquiries and complaints from employees in relation to their health information being inappropriately collected or disclosed, or not being stored securely.[46]

36.28 The Mental Health Legal Centre expressed concern about the release of information about a person's mental health to prospective employers. It submitted that:

> We know anecdotally of many situations when a person has become unwell, taken leave and produced a medical certificate with the reason for their absence with a diagnosis of their illness. These medical reports go on their employment file and may (and do) mean that a prior knowledge of the person's mental health affects future jobs options.[47]

36.29 In addition, the Mental Health Legal Centre stated that:

> People found not guilty on the grounds of mental impairment under the Victorian *Crimes Mental Impairment and Unfitness to be Tried Act* (1998) have such findings recorded on LEAP (police data). This information is released to potential employers by police upon request (and consent signed by the employee).[48]

36.30 Some stakeholders observed that a significant number of the complaints closed by the OPC as falling outside its jurisdiction concerned the employee records exemption.[49] It was also submitted that 'experience in other jurisdictions (including the IPP regime applying to Commonwealth agencies) shows that employees are major users of privacy rights'.[50]

---

44 ACTU, *Submission PR 155,* 31 January 2007.

45 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Mental Health Legal Centre Inc, *Submission PR 184,* 1 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

46 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

47 Mental Health Legal Centre Inc, *Submission PR 184,* 1 February 2007.

48 Ibid.

49 See, eg, Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

50 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

36.31 Several stakeholders observed that there is privacy protection for employee records of public sector employees but not for those employed in the private sector.[51] For example, the Victorian Government stated:

> under the *Privacy Act* the personal information of workplace participants receives differential treatment depending upon their employment status, and whether or not they work in the public or private sectors. With the increasing mobility of the workforce and increased use of contractors in the workplace, there appears to be no justification for this differential treatment.[52]

36.32 This differential treatment is highlighted by the handling of employee records by Australian Government agencies that are subject to the IPPs in relation to their non-commercial activities and the NPPs in relation to their commercial activities, such as the Australian Postal Corporation. In its submission, the Australian Postal Corporation stated that

> staff who are employed by Australian Post in connection with its commercial activities do not have the same rights of access to their employment records under the law as their colleagues who are employed by the Corporation with its non-commercial activities.[53]

36.33 The OPC submitted that the removal of the employee records exemption would improve the consistent application of the privacy principles to both the public and private sectors.

36.34 The ACTU suggested that it seems unethical for a business to handle the personal information of customers and suppliers differently from that of their employees.[54]

> The moral case for employers being required to respect the confidentiality of information acquired by them about their employees in the course of the latter's employment seems unassailable. It is consistent with the common law duty of trust and confidence which courts have found employers to owe their employees, including in respect of information provided by employees.[55]

36.35 Some stakeholders noted gaps in the protection of workers' privacy in legislation[56] and, in particular, the limited protection provided by the workplace

---

51 Government of Victoria, *Submission PR 288,* 26 April 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Australia Post, *Submission PR 78,* 10 January 2007.

52 Government of Victoria, *Submission PR 288,* 26 April 2007.

53 Australia Post, *Submission PR 78,* 10 January 2007.

54 ACTU, *Submission PR 155,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007.

55 ACTU, *Submission PR 155,* 31 January 2007.

56 Law Institute of Victoria, *Submission PR 200,* 21 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; ACTU, *Submission PR 155,* 31 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

relations legislation.[57] It was also suggested in some submissions that the continuation of the exemption is likely to lead to further fragmentation in states that have enacted legislation regulating the area of workplace privacy.[58] Some stakeholders noted with concern that states are introducing legislation that attempts to deal with a perceived gap in privacy protection for employees, which results in the complexity of complying with multiple state-based legislation. These stakeholders were of the view that, in the interests of national consistency, the *Privacy Act* should apply to the personal information of employees in place of existing state legislation in this area.[59] Telstra submitted that large companies are covered by state and federal privacy legislation and have the additional burden of 'an unreasonably high cost of compliance in order to comply with several differing privacy regimes relating to employees'.[60]

36.36 The OPC stated that removing the exemption could have a number of benefits, including:

- offering an appropriate balance between the interests of the parties, just as it offers such a balance between organisations and their customers
- providing a minimum set of standards for privacy protection of employee records, consistent with protection of an employee's rights as a private citizen
- providing certainty about rights and obligations for employers and employees
- eliminating regulatory difficulties in interpreting the exemption
- providing access to a conciliation-based complaints process through the Office of the Privacy Commissioner.[61]

36.37 Some stakeholders submitted that the additional costs of compliance resulting from any proposed removal of the exemption may be mitigated by certain factors.[62] The OPC submitted:

> The Office understands that many large businesses already apply the privacy principles to their handling of employee records. For those businesses any removal of the exemption may not create an added compliance cost. Conversely for those

57 Law Institute of Victoria, *Submission PR 200,* 21 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

58 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

59 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

60 Telstra, *Submission PR 185,* 9 February 2007.

61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

62 Ibid; AAMI, *Submission PR 147,* 29 January 2007.

> businesses that do not currently apply the NPPs to their employee records there would be costs to implement and maintain a compliance regime.[63]

36.38 Similarly, AAMI submitted that

> in practice (for larger businesses at least) procedures have been implemented to ensure that employee information is treated in the same way as all other personal information/sensitive information that is received.[64]

36.39 The Office of the Information Commissioner Northern Territory submitted that 'in the absence of clear evidence to the contrary, … the extent of the additional costs to business of removal of the employee records exemption should not be assumed or overstated'. The Office stated that the increase in resources required to include private sector employee records within the existing scheme may be 'marginal', on the basis that:

- because information about clients is not exempted, most businesses subject to the Act are already required to have in place: mechanisms for developing policies to implement the NPPs; and procedures for dealing with complaints about breaches of the NPPs;
- there is growing expertise in dealing with privacy issues within the workforce because of the extensive coverage of privacy legislation. [65]

36.40 It was also submitted that simplifying the structure of the *Privacy Act* by removal of the exemption would remove the current costs of interpreting and applying the employee records exemption.[66]

36.41 Furthermore, some stakeholders submitted that compatibility with overseas jurisdictions and international standards should be a factor in considering whether the exemption should remain.[67] The New Zealand Privacy Commissioner noted the desirability of trans-Tasman compatibility, which may be facilitated by, for example, 'a seamless application of privacy protections for the information of prospective employees applying for work in the other country', or 'former employees after they return home'.[68]

36.42 Professor Graeme Greenleaf, Nigel Waters and Associate Professor Lee Bygrave noted that the Article 29 Working Party has expressed concern that human resource data are often traded across borders and often contain sensitive information.

---

63 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
64 AAMI, *Submission PR 147,* 29 January 2007.
65 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
66 Ibid.
67 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; New Zealand Privacy Commissioner, *Submission PR 128,* 17 January 2007.
68 New Zealand Privacy Commissioner, *Submission PR 128,* 17 January 2007.

Although there is no empirical data on the quantity and nature of information flows from Europe to Australia,

> there can be little doubt that personal data *are* being transferred along this channel and that at least some of these relate to current or past employment matters, and are, in addition, sensitive.[69]

Retention of the exemption

36.43 A number of stakeholders expressed support for the retention of the employee records exemption.[70] Some stakeholders suggested that there has been no evidence of detriment caused by the exemption.[71] DEWR stated that submissions to the AGD and DEWR discussion paper on employee records privacy 'did not disclose any significant detriment caused by the employee records exemption that warranted changing the *status quo* and imposing additional compliance costs on business'.[72] Similarly, the Australian Chamber of Commerce and Industry (ACCI) submitted that:

> In the few years the legislation has been in place, there has been no evidence of any systemic problems or shortcomings with the exemption. The onus should be on those parties who wish to alter the current status quo to provide evidence that the exemption should be removed.[73]

36.44 Abacus–Australian Mutuals (Abacus) submitted that it was 'not aware of any substantive concerns in relation to this exemption and therefore believes it should remain on foot'.[74] UNITED Medical Protection, while supportive of the principle of privacy protection for employees, submitted that IP 31 did not indicate that employers are not maintaining the privacy of employees' personal information or denying them access to such information.[75]

---

69 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

70 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

71 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

72 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007, referring to Australian Government Attorney-General's Department and Australian Government Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (2004).

73 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

74 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

75 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

36.45 Some stakeholders noted the original opposition by businesses to the inclusion of employee records in the private sector provisions of the *Privacy Act*.[76] The ACCI submitted that the employee records exemption 'was a key factor in industry supporting the extension of Commonwealth privacy legislation to the private sector in 2001' and that any removal or narrowing of the exemption 'would necessitate a re-evaluation by industry of support for privacy regulation in the private sector'.[77]

36.46 It was suggested in some submissions that the removal of the exemption would result in an additional regulatory burden and an increase in the costs of compliance for businesses.[78] The ACCI stated that it

> continues to receive advice from member organisations that the exemption is required to assist employers to manage and run their businesses effectively, both in terms of real costs and time.[79]

36.47 The ACCI submitted that any removal or modification of the exemption would: impose substantial costs on businesses; create operational human resource management problems, particularly if other provisions of the Act are modified; and lead to a restriction of business activity, which ultimately would impact adversely on business profitability and the ability of businesses to hire employees.[80]

36.48 The Australian Bankers' Association (ABA) submitted that 'abolition of the employee records exemption would potentially impose a layer of additional record keeping costs and cut across the way banks currently handle employee issues'.[81] The Australian Retailers Association stated 'by adding a further set of employee records principles in the *Privacy Act* it would become heavily regulated, time consuming and costly for employers, especially small businesses'.[82] Abacus submitted that:

> Removing the exemption has the capacity to add significantly to internal systems costs and compliance checks without appreciable benefit to employees and would be likely to impact particularly on smaller businesses.[83]

36.49 Some stakeholders submitted that, despite the exemption, employers already handle employee records with care.[84] The ABA stated that 'each member bank has its

---

76 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

77 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

78 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

79 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

80 Ibid.

81 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

82 Australian Retailers Association, *Submission PR 131,* 18 January 2007.

83 Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007.

84 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

own policies and practices in relation to the keeping, maintenance and control of and access to its employees' records'.[85] UNITED Medical Protection submitted that their human resources department operates on the basis of preserving employees' confidentiality.[86] Similarly, the ACCI stated that:

> Notwithstanding the exemption, employers treat information gathered during the employment relationship with due sensitivity, care and protection. …
>
> It should be noted that business has a serious concern for the protection of sensitive information, such as employee records. It would be erroneous to conclude that just because an exemption exists that employers do not take adequate and conscientious safeguards to protect this data from misuse or exploitation.[87]

36.50 Both the ACCI and the Australian Retailers Association contended that the current workplace relations legislation provides sufficient privacy protection for employees.[88] The ACCI stated that:

> The *Workplace Relations Act 1996* and similar State and Territory legislation extensively regulates record keeping of certain employee records with a well resourced inspectorate. The regime also has the ability to impose substantial penalties for non-compliance.[89]

36.51 In addition, the ACCI submitted that other reasons for the employee records exemption are that: employers maintain employment records mostly for the purposes of complying with statutory requirements that seek to protect the interests of employees; and the maintenance of such records is an essential consequence of the employment relationship and 'does not involve any invasion of privacy or unlawfulness'. It also took the view that:

> Employers continue to operate under a range of regulatory systems, many of which are difficult to comply with. Changes to the exemption should not be contemplated at the present time, particularly when employers and employees alike are adjusting to a major reform in the workplace relations system with the passage of the WorkChoices legislation.[90]

36.52 The Australian Retailers Association, while acknowledging that 'employee information does require privacy protection', submitted that 'abolishing the employee records exemption within the *Privacy Act* will only increase the confusion and intricacies of the Act'.[91] The ACCI expressed concern that:

> State and Territory privacy legislation is not consistent with the Commonwealth Act and ultimately leads to uncertainty. ACCI advocates that an employee records

---

85 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.
86 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.
87 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
88 Ibid; Australian Retailers Association, *Submission PR 131,* 18 January 2007.
89 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
90 Ibid.
91 Australian Retailers Association, *Submission PR 131,* 18 January 2007.

> exemption is so fundamental that it should not only be retained, but also applied at the State and Territory level.[92]

36.53 AXA submitted that the employee records exemption should be retained, because disputes between employers and employees often include non-privacy related issues that cannot be dealt with by the Privacy Commissioner. AXA submitted that removing the employee records exemption is 'likely to further "segment" disputes which need a more holistic approach'.[93]

36.54 Another concern raised was the need of potential purchasers of businesses to have access to employee records. The ACCI submitted that any proposed removal of the exemption 'would substantially interfere with a purchaser's ability to conduct due diligence when buying a business, including whether it is financially viable to retain existing staff'. It was suggested that potential buyers need to be able to access vendor records, including employee records, in order to determine whether they would buy the business, retain existing staff and seek funds transfer for the vendor. The ACCI submitted that the employee records that would be relevant in this context include records that: indicate the level of leave entitlement; reveal potential issues concerning occupational health and safety or workers compensation; and concern employees' conduct that may give rise to potential legal actions, such as unfair dismissal or anti-discrimination suits.[94]

36.55 Both DEWR and the ACCI supported the use of non-binding best practice guidelines instead of legislation.[95] DEWR stated that if there is to be a change in the regulatory approach towards employee records privacy, 'guidelines are likely to be met with greater support from employer groups'.[96] The ACCI also supported 'the formulation of educational initiatives to better inform employers and employees of their rights and obligations regarding employee records'.[97]

ALRC's view

36.56 Employee records can contain a significant amount of personal information about employees, including sensitive information such as health and genetic information. There is a real potential for individuals to be harmed if employees' personal information is used or disclosed inappropriately. The lack of adequate privacy protection for employee records in the private sector is of particular concern because employees may be under economic pressure to provide personal information to their employers.

---

92 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
93 AXA, *Submission PR 119,* 15 January 2007.
94 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
95 Ibid; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
96 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
97 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

36.57 Although there is no empirical evidence of misuse of information on employee records, the ALRC notes that the OPC received a large number of inquiries that related to this exemption. The Victorian Office of the Health Services Commissioner also submitted that it has received many inquiries and complaints from employees about their health information being misused or stored insecurely.

36.58 In the ALRC's view, there is no sound policy reason why privacy protection for employee records is only available to public sector employees and not private sector employees. Treating employees' personal information differently from other personal information is also unjustifiable.

36.59 At the time the private sector provisions of the *Privacy Act* were introduced, the Australian Government acknowledged that employee records deserve privacy protection but considered that the issue would be more appropriately dealt with in workplace relations legislation. Six years after the enactment of the private sector provisions, however, workplace relations legislation still does not provide sufficient privacy protection for employee records.

36.60 In the ALRC's view, multi-layered privacy regulation is not a reasonable justification to avoid putting in place privacy protection for employee records. Moreover, maintaining the employee records exemption may result in further regulation by states and territories, thus contributing to fragmentation and inconsistency in workplace privacy regulation.

36.61 Advocates of the exemption suggested in submissions that the costs of compliance are the main reason for retaining the exemption. The ALRC is, however, not persuaded that such costs provide a sufficient policy basis to support the exemption. In addition, the costs to businesses resulting from the removal of the exemption should not be overestimated. In considering the costs of compliance, it should be borne in mind that the organisations which will carry the greatest burden—that is, large businesses—are already required to comply with the *Privacy Act* and therefore already have in place mechanisms and procedures for the handling of personal information. It was also indicated in submissions that some businesses already treat employee records the same way they treat other personal information.

36.62 Furthermore, privacy legislation in some comparable overseas jurisdictions, such as the United Kingdom and New Zealand, does not contain an exemption that applies to employee records. The removal of the employee records exemption may also facilitate recognition of the adequacy of Australian privacy law by the EU, and trade with EU organisations.

36.63 For these reasons, the ALRC is of the view that the privacy of employee records requires regulation and proposes that the employee records exemption be removed. The removal of the exemption would ensure that the privacy of employee records held by

organisations is protected under the *Privacy Act*, and that employees' sensitive information, such as health and genetic information, is given a higher level of protection under the Act. This protection should be in addition to the relevant provisions in the *Workplace Relations Regulations*.

36.64 In Chapter 3, the ALRC proposes that the definition of 'sensitive information' in the *Privacy Act* be amended to include biometric information collected for the purpose of automated biometric authentication or identification as well as biometric template information. Therefore, such biometric information handled in the context of private sector employment will also be given the same level of privacy protection as other sensitive information.

Proposal 36–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.

Evaluative material

36.65 The 2000 House of Representatives Committee inquiry acknowledged that there is a difference between an employee's health, family and financial information, which should not be provided to anyone else without the consent of the employee; and information concerning disciplinary matters or career progression of the employee.[98] The inquiry went on to recommend a significant narrowing of the scope of the exemption to apply only to 'exempt employee records', which would consist of records relating to: the engagement, training, disciplining or resignation of the employee; termination of employment; and the employee's performance or conduct.[99]

36.66 The 2000 House of Representatives inquiry recommended that the other matters listed in the proposed definition of 'employee record' be subject to the NPPs. It also noted that employee records can contain personal and sensitive information regardless of the size of the employer and therefore was of the view that its recommendations also should apply to small business employers.[100] The inquiry's recommendations were not intended to override the provisions in the workplace relations legislation.[101] The inquiry's recommendations were rejected by the Australian Government.[102]

98 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.36].
99 Ibid, recs 5–7.
100 Ibid, [3.40].
101 Ibid, [3.39].
102 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

Submissions and consultations

36.67 In IP 31, the ALRC asked what the scope of the employee records exemption should be if the exemption were to remain.[103] Advocates of the exemption strongly objected to limiting the scope of the exemption.[104] For example, the ACCI was of the view that the exemption is 'extremely limited in its scope and the circumstances to which it applies' and did not support any proposal to weaken the exemption.[105] DEWR stated that:

> It was also generally felt that varying the scope of the exemption, for instance, by retaining some of the NPPs for employee records or restricting the exemption by excluding sensitive information from it, would only contribute to the complexity of the privacy framework.[106]

36.68 Other stakeholders submitted that although there should be no general exemption for employee records, some uses of employment records in particular contexts may justify exemptions from, or modifications to, particular privacy principles,[107] provided that the exceptions are specified as narrowly as reasonably possible.[108] For example, the Victorian Office of the Health Services Commissioner submitted that the employee records exemption should be limited to 'the engagement, disciplining and termination of employment as well as the employee's performance or conduct', including, for example, reference checks by prospective employers.[109]

36.69 Stakeholders were also concerned that the proposed changes to the scope of the employee records exemption may affect the ability of prospective employers to engage in free and frank discussion with referees.[110] The ACCI stated that businesses need to be able to ascertain a job applicant's work history (such as disciplinary matters, warnings and terminations) and work experience at the recruitment stage to be confident that that the candidate has the requisite skill and aptitude for the relevant role. It stated that this information is particularly important where the candidate may be working with vulnerable people or applying for a position of trust.[111]

---

103 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–9.
104 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
105 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.
106 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
107 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
108 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
109 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.
110 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; M Hunter, *Submission PR 16,* 1 June 2006.
111 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

36.70 The ACCI further submitted that legally requiring employers to obtain the consent of candidates to perform routine reference checks before hiring would result in delays in the recruitment process, or selecting the wrong candidate for the job.[112] In addition, the ACCI suggested that, since the exemption does not preclude legal actions for anti-discrimination or unlawful termination, the potential for discrimination against an employee due to access to employee records should not be a reason for removing the exemption.[113]

36.71 UNITED Medical Protection submitted that there should be categories of information exempt from access by an employee. It suggested that, for example, employees should be able to access evaluative records such as their own performance reviews, but not employment references.

> If employees were able to access records relating to employment references this would very likely see a dramatic reduction in the willingness of past employers and other relevant persons to provide references due to the threat of litigation by the employee if the employee accessed the record containing the reference and did not agree with the comments made by the person providing the reference. This would be counter to the interests of prospective employers and also the interests of most employees.[114]

36.72 In contrast, the Legal Aid Commission of New South Wales submitted that 'many workers have concerns about the adverse effects of unfair referee reports that may be an obstacle to their continued employment'.[115]

36.73 DEWR stated that, if a more prescriptive framework for the protection of employee records is proposed, 'consideration should be given to achieving this with the least inconvenience to business', for example, by:

> safeguarding the employer's right to refuse an employee's access to their records in certain circumstances; minimising the impact of the more onerous privacy principles such as the notice requirements in NPP 1.3; and ensuring a substantial transition period before business are required to comply.[116]

36.74 The Australian Government Department of Human Services submitted that 'it may be useful to consider the potential impact on smaller organisations that only collect, hold and use health information pertaining exclusively to their employees'.[117]

Options for reform

36.75 As discussed above, the ALRC proposes the removal of the employee records exemption. The ALRC acknowledges the concern expressed by some stakeholders that

---

112 Ibid.
113 Ibid.
114 UNITED Medical Protection, *Submission PR 118,* 15 January 2007.
115 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
116 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
117 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

the removal of the exemption may affect the ability of prospective employers to engage in full and frank discussion with a job applicant's previous employer. In order to address that concern, three options for reform may be considered.

36.76 One option is to exclude personal references given by referees from the operation of the *Privacy Act*. The Canadian *Privacy Act 1985* defines 'personal information' to exclude 'the personal opinions or views of the individual … about another individual'.[118]

36.77 Another option is to amend the *Privacy Act* to allow the recipient of the reference to deny a request for access to a reference that is given to it in confidence. Under s 29 of the *Privacy Act 1993* (NZ), an agency may deny a request for access to evaluative material, disclosure of which would breach a promise of confidence to the supplier of the information. 'Evaluative material' is defined to mean:

> evaluative or opinion material compiled solely—
>
> (a) For the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates—
>
> (i) For employment or for appointment to office; or
>
> (ii) For promotion in employment or office or for continuance in employment or office; or
>
> (iii) For removal from employment or office; or
>
> (iv) For the awarding of contracts, awards, scholarships, honours, or other benefits; or
>
> (b) For the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or
>
> (c) For the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.[119]

36.78 A third option is to allow a potential employer to deny access to a personal reference given by a referee until after the job applicant has been informed of the result of the recruitment process. In Hong Kong, s 56 of the *Personal Data (Privacy) Ordinance* provides that unless the referee consents, a data user does not have to provide a job applicant with access to, or a copy of, a personal reference given by the referee until after the job applicant has been informed in writing that he or she has been accepted or rejected to fill that position or office.[120]

---

118 *Privacy Act* RS 1985, c P-21 (Canada) s 3.

119 *Privacy Act 1993* (NZ) s 29(3).

120 *Personal Data (Privacy) Ordinance* (Hong Kong) s 56.

ALRC's view

36.79 Stakeholders emphasised that any proposed removal of the employee records exemption should take into account the need of prospective employers to engage in full and frank discussion with previous employers about an employee. The ALRC is of the view that there is sufficient ground for an exception to the access principle, provided that a personal reference is given in confidence to a potential employer. This is in line with the common law obligation of confidence. At common law, an action for breach of confidence may arise where:

- the information has the 'necessary quality of confidence'—that is, it must be non-trivial, and, to some extent, secret or inaccessible;
- the information was communicated or obtained in such circumstances as to give rise to an obligation of confidence; and
- there is actual or threatened unauthorised use of the information.[121]

36.80 Such an exception is also in line with the law that is currently applicable to employees of Australian Government agencies. Although employment records of an Australian Government agency employee are covered by *Privacy Act*, the employee may not be entitled to access personal references about him or her held by an agency if its disclosure would found an action for breach of confidence.[122]

36.81 Accordingly, the ALRC proposes that the *Privacy Act* provide for an exception to the proposed 'Access' principle in relation to a request for access to 'evaluative material' that is given in confidence to an agency or organisation. The proposed amendment should be based on the approach taken in the New Zealand *Privacy Act 1993*. This allows an agency or organisation to deny a request for access by a job applicant to confidential evaluative materials complied solely for the purpose of determining the job applicant's suitability for employment or appointment to a position. This model is preferable to one that excludes personal references from the operation of all privacy principles, because exceptions to the proposed Unified Privacy Principles should be as narrowly drawn as possible. In addition, since the common law obligation of confidence endures for the duration of the confidential relationship, the ALRC does not consider that the exception should apply only until the end of the recruitment process.

---

121 *Moorgate Tobacco Co Ltd v Philip Morris Ltd [No 2]* (1984) 156 CLR 414, 438.

122 Under Information Privacy Principle (IPP) 6, a public sector agency may refuse a request by an individual for access to personal information that the agency holds to the extent that the agency is required or authorised to refuse access under an applicable Commonwealth law that provides for access by persons to documents: *Privacy Act 1988* (Cth) s 14 IPP 6. Under the *Freedom of Information Act 1982* (Cth), an agency may refuse to grant access to the documents if their disclosure under the Act would found an action by a person for breach of confidence: *Freedom of Information Act 1982* (Cth) ss 11, 45.

36.82 In the ALRC's view, the same exception that applies to confidential personal references should also apply to evaluative material complied for the sole purpose of determining the awarding, continuation, modification or cancellation of contracts, awards, scholarships, honours or other benefits. This is because in determining whether an individual should be awarded a contract, an award or other similar benefits, the referee should be able to provide an honest evaluation about the individual's merits without fear of that evaluation being made available to the individual concerned.

36.83 Another concern raised was the need for prospective purchasers of a business to have access to employee records in conducting due diligence. The ALRC is of the view that no exception or exemption in this context is warranted. Where the disclosure of an employee record by the vendor organisation is necessary to enable the prospective purchaser to assess whether to employ particular individuals from the vendor organisation, the individuals' consent for the disclosure should be obtained. In other circumstances, the disclosure of aggregate information about an organisation's employees may be adequate for due diligence purposes.[123]

Proposal 36–2 The *Privacy Act* should be amended to provide that an agency or organisation may deny a request for access to evaluative material, disclosure of which would breach an obligation of confidence to the supplier of the information. 'Evaluative material' for these purposes means evaluative or opinion material compiled solely for the purpose of determining the suitability, eligibility, or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit.

Location of privacy provisions concerning employee records

36.84 If the employee records exemption were to be removed or modified, a further issue is whether privacy provisions should be located in the *Privacy Act*, workplace relations legislation or elsewhere. The 2005 Senate Committee privacy inquiry was of the view that the most appropriate place to protect employee privacy is in the *Privacy Act* rather than in workplace relations legislation. Further, the inquiry considered that attempts by state governments to regulate workplace surveillance would only

123 The Privacy Commissioner has issued guidance on the application of the NPPs to the buying and selling of businesses. The Privacy Commissioner noted that there are some circumstances in which the employee records exemption may apply, but 'encourage[d] vendor organisations always to consider whether disclosure of aggregated information relating to their employees is adequate for due diligence purposes regardless of whether the exemption might apply': Office of the Federal Privacy Commissioner, *Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*, Information Sheet 16 (2002).

contribute to problems of inconsistency and fragmentation. It therefore recommended that the privacy of employee records be protected under the *Privacy Act*.[124]

Submissions and consultations

36.85 In IP 31, the ALRC asked where the employee records exemption should be located—in the *Privacy Act*, workplace relations legislation or elsewhere—if the exemption were to remain.[125] Some stakeholders submitted that the appropriate location for exemption is in privacy legislation,[126] on the basis that this: has worked well in the *Privacy Act*;[127] would allow users of the Act to assess their responsibilities and obligations properly; and would promote national consistency.[128]

36.86 It was suggested in some submissions that the exemption should not be located in the *Workplace Relations Act,* because that Act does not have universal application,[129] and relocating the exemption to that Act would raise unrelated workplace relations concerns.[130]

36.87 In contrast, some stakeholders submitted that privacy regulation concerning employees' personal information should be addressed in workplace relations legislation.[131] The Australian Government Department of Human Services considered that the employee records exemption is 'more relevant' to workplace relations legislation.[132] AXA submitted that:

> The employer/employee relationship is already subject to significant regulation; any regulation in relation to privacy and access should be addressed in the legislation dealing specifically with employment.[133]

36.88 Other stakeholders submitted that provisions concerning employees' rights, especially in relation to workplace privacy, should be contained in a single legislative instrument.[134] AAPT submitted that all employee-related rights should be incorporated into a single legislative instrument, because separate legislative regimes and overlapping legislation (including state-based workplace surveillance and telecommunications interception legislation) created confusion and made the task of

---

124 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.36]–[7.37], rec 13.

125 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–9.

126 ACTU, *Submission PR 155,* 31 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

127 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

128 UNITED Medical Protection, *Submission PR 118,* 15 January 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

129 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007; Victorian Automobile Chamber of Commerce, *Submission PR 100,* 15 January 2007.

130 Australian Chamber of Commerce and Industry, *Submission PR 219,* 7 March 2007.

131 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007; AXA, *Submission PR 119,* 15 January 2007.

132 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

133 AXA, *Submission PR 119,* 15 January 2007.

134 Law Institute of Victoria, *Submission PR 200,* 21 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007; AAPT Ltd, *Submission PR 87,* 15 January 2007.

compliance onerous—'potentially lessening the protection that is otherwise afforded by the existence of these Acts'.[135] Similarly, the Law Institute Victoria stated that:

> It would be desirable for all aspects of workplace privacy including information privacy to be regulated in the one piece of legislation, provided a consistent approach was adopted across the States and Territories.
>
> However, in the absence of such legislation, the LIV favours clear, easy to follow provisions in relation to employee records at a national level.[136]

ALRC's view

36.89 The existence of the employee records exemption only increases the level of complexity of the *Privacy Act*. Introducing a further set of privacy principles in a different piece of legislation such as the *Workplace Relations Act* is unlikely to reduce the complexity of the privacy regime.[137]

36.90 The ALRC is of the view that privacy protection of employee records should be located in the *Privacy Act* to allow maximum coverage of agencies and organisations and to promote consistency. Provisions regulating the privacy of employee records should not be located in workplace relations legislation because the *Workplace Relations Act* only applies to specified persons or entities, such as constitutional corporations and persons or entities that engage in constitutional trade and commerce.[138] In addition, employee records are no different from other personal information and therefore should be regulated under the *Privacy Act* in the same way as other personal information.

---

135 AAPT Ltd, *Submission PR 87,* 15 January 2007.

136 Law Institute of Victoria, *Submission PR 200,* 21 February 2007.

137 See Australian Law Reform Commission, *Submission to the Australian Government Attorney-General's Department of Employment and Workplace Relations Review on Employee Records Privacy*, 8 April 2004.

138 The *Workplace Relations Act 1996* (Cth) only applies to specified persons or entities that employs, or usually employs, an individual. The specified persons or entities include: a constitutional corporation; the Australian Government; Australian Government authorities; a person or entity (which may be an unincorporated club) that employs (or usually employs), in connection with constitutional trade or commerce, an individual as a flight crew officer, a maritime employee, or a waterside worker; a body corporate incorporated in an Australian territory; and a person or entity (which may be an unincorporated club) that carries on an activity in an Australian territory in Australia: *Workplace Relations Act 1996* (Cth) s 6(1).

37. Political Exemption

Contents

Introduction 1065
Current law 1065
Registered political parties, and political acts and practices 1065
Ministers 1068
Government inquiries 1069
International instruments 1070
Electoral databases 1071
Implied freedom of political communication 1072
Submissions and consultations 1073
Registered political parties 1073
Political acts and practices 1075
Ministers 1077
ALRC's view 1077

Introduction

37.1 The *Privacy Act 1988* (Cth) (*Privacy Act*) does not apply to registered political parties, or political representatives engaging in certain activities in the political process. This exemption is usually referred to as the political exemption. In addition, Australian Government ministers are generally only required to comply with the *Privacy Act* when they are acting in an official capacity. This chapter examines whether the political exemption and the exemption that applies to Australian Government ministers should remain.

Current law

Registered political parties, and political acts and practices

37.2 A 'registered political party' is specifically excluded from the definition of 'organisation' and is therefore exempt from the operation of the *Privacy Act*.[1] In

1 *Privacy Act 1988* (Cth) s 6C(1). A 'registered political party' means a political party registered under Part XI of the *Commonwealth Electoral Act 1918* (Cth): *Privacy Act 1988* (Cth) s 6(1). A list of registered political parties is available on the Australian Electoral Commission's website: Australian Electoral Commission, *Current List of Political Parties* (2007) <www.aec.gov.au/Parties_and_Representatives/Party_Registration/index.htm> at 24 July 2007.

addition, political acts and practices of certain organisations are also exempt.[2] These organisations include: political representatives—namely, Members of Parliament and local government councillors; contractors and subcontractors of registered political parties and political representatives; and volunteers for registered political parties.[3] Acts and practices covered by the exemption include elections held under an electoral law;[4] referendums held under a law of the Commonwealth, a state or a territory; and participation by registered political parties and political representatives in other aspects of the political process.[5]

37.3 In addition to the exemption under the *Privacy Act*, there are other legislative provisions that specifically permit the collection and use of personal information by registered political parties and political representatives in certain circumstances. Under s 90B of the *Commonwealth Electoral Act 1918* (Cth), the Electoral Commission must give information in relation to electoral rolls and certified lists of voters to specified persons or entities in certain circumstances.[6] The persons and entities that are entitled to this information include candidates for a House of Representatives election, registered political parties, Members of Parliament, and state and territory electoral authorities.[7]

37.4 Members of Parliament and political parties may only use the information for certain permitted purposes, including: any purpose in connection with an election or referendum; research regarding electoral matters; monitoring the accuracy of information in electoral rolls; and the performance by Members of Parliament of their functions as parliamentarians concerning enrolled persons.[8] Section 91B of the *Commonwealth Electoral Act* makes it an offence to use the information obtained under the Act for commercial purposes.

37.5 Registered political parties and political representatives are exempt from legislation dealing with some aspects of telemarketing. Under the *Do Not Call Register Act 2006* (Cth), registered political parties, independent Members of Parliament and electoral candidates are exempt from the prohibition against making unsolicited telemarketing calls to a number registered on the Do Not Call Register, provided the call is made for certain specified purposes. The specified purposes include: conducting

---

2 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7C.

3 Ibid s 7C.

4 An 'electoral law' means a Commonwealth, state or territory law relating to elections to a Parliament or to a local government authority: Ibid s 7C(6).

5 Ibid s 7C.

6 The electoral roll sets out each elector's surname, Christian or given names, and place of living. Addresses are suppressed for eligible overseas and itinerant electors: *Commonwealth Electoral Act 1918* (Cth) s 83. A certified list of voters includes each voter's name, sex and date of birth: *Commonwealth Electoral Act 1918* (Cth) s 208.

7 Where the Electoral Commission provides a copy of the electoral roll to a registered political party, a state or territory senator or a member of the House of Representatives, it may also provide certain additional information about electors, including, among other things, an elector's postal address, sex, date of birth, salutation and enrolment status: *Commonwealth Electoral Act 1918* (Cth) s 90B(2).

8 Ibid s 91A.

fundraising for electoral or political purposes; and where the call relates to goods or services, the caller is the supplier or prospective supplier of the goods or services.[9]

37.6 Registered political parties are also exempt from legislation dealing with some aspects of email marketing. Under the *Spam Act 2003* (Cth), registered political parties may, without the prior consent of the recipient, send 'designated commercial electronic messages' that are purely factual or in respect of goods or services that the parties directly supply. Such messages must include information about the individual or organisation that authorised the sending of the message, but they do not have to contain a functional unsubscribe facility.[10]

37.7 In its review of the operation of the *Spam Act* in 2006, the Australian Government Department for Communications, Information Technology and the Arts (DCITA) rejected proposals to extend the coverage of the *Spam Act* to non-commercial messages, on the basis that: such an extension may have an adverse impact on political and religious freedoms; and unsolicited contact that is non-commercial in nature 'is not currently a significant problem relative to commercial spam'. DCITA stated that the provisions concerning designated electronic commercial messages should be maintained as a safeguard for the activities of those who are exempt from the *Spam Act*.[11]

37.8 In his second reading speech on the Privacy Amendment (Private Sector) Bill 2000 (Cth), the then Attorney-General, Mr Daryl Williams AM QC MP, stated that:

> Freedom of political communication is vitally important to the democratic process in Australia. This exemption is designed to encourage that freedom and enhance the operation of the electoral and political process in Australia. I am confident that it will not unduly impede the effective operation of the legislation.[12]

37.9 At the time of the introduction of the Bill, the Privacy Commissioner stated that he did not think that the exemption for political organisations was appropriate.[13]

> If we are to have a community that fully respects the principles of privacy and the political institutions that support them, then these institutions themselves must adopt

---

9 *Do Not Call Register Act 2006* (Cth) s 11, sch 1 cls 2–3. Under this Act, a 'registered political party' means a political party, or a branch or division of a political party, registered under either the *Commonwealth Electoral Act 1918* (Cth) or a state or territory law that deals with electoral matters: *Do Not Call Register Act 2006* (Cth) s 4. The *Do Not Call Register Act* is discussed further in Ch 64.

10 *Spam Act 2003* (Cth) ss 16–18, sch 1 cl 3(a)(ii). Under this Act, a 'registered political party' means a political party, or a branch or division of a political party, registered under either the *Commonwealth Electoral Act 1918* (Cth) or a state or territory law that deals with electoral matters: *Spam Act 2003* (Cth) s 4. The *Spam Act* is discussed further in Ch 64.

11 Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006), 6, 29–30, 69.

12 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15753.

13 M Crompton (Federal Privacy Commissioner), 'Media Release: Federal Privacy Commissioner, Malcolm Crompton Comments on Private Sector' (Press Release, 12 April 2000).

> the principles and practices they seek to require of others. I believe that political organisations should follow the same practices and principles that are required in the wider community.[14]

37.10 In June 2006, Senator Natasha Stott Despoja introduced a Private Member's Bill to remove the exemption for political acts and practices.[15] In her second reading speech she stated that:

> Politicians should be included in the rules that we expect the public and private sectors to abide by. We cannot lead and represent Australians when we do not adhere to the rules that we have made for them, as this merely plays into the notion that politicians cannot be trusted.[16]

37.11 For the period from 21 December 2001 to 31 January 2005, the Office of the Privacy Commissioner (OPC) stated that 0.4% of all the National Privacy Principle (NPP) complaints closed by the Office as outside its jurisdiction concerned the political exemption.[17]

37.12 A number of overseas jurisdictions, including the United Kingdom, Canada, New Zealand and Hong Kong, do not provide for an exemption of political parties or political acts and practices from their privacy legislation.

Ministers

37.13 The *Privacy Act* applies to Australian Government ministers only where their acts and practices relate to the affairs of agencies, 'eligible case managers'[18] or 'eligible hearing service providers';[19] or where the acts and practices are in relation to a record concerning these affairs that is in the ministers' possession in their official

---

14 Ibid.

15 Privacy (Extension to Political Acts and Practices) Amendment Bill 2006 (Cth). At the time of writing, the Bill has been read for the second time in the Senate.

16 Commonwealth, *Parliamentary Debates*, Senate, 22 June 2006, 19 (N Stott Despoja). The Australian Democrats also unsuccessfully attempted to introduce amendments to the Do Not Call Register Bill 2006 (Cth) to prevent politicians from making telemarketing calls: Commonwealth, *Parliamentary Debates*, Senate, 21 June 2006, 25 (N Stott Despoja). The *Do Not Call Register Act 2006* (Cth) is discussed in Ch 33.

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

18 The Information Privacy Principles (IPPs) apply to the acts and practices of 'eligible case managers' in connection with the provision of case management services or the performance of their functions under the *Employment Services Act 1994* (Cth): *Privacy Act 1988* (Cth) ss 6(1), 7(1)(cb). An 'eligible case manager' is an entity that is or has been a contracted case manager within the meaning of the *Employment Services Act*: *Privacy Act 1988* (Cth) s 6(1). Although the *Employment Services Act* was repealed in April 2006, the *Privacy Act 1988* (Cth) continues to provide privacy protection in relation to acts and practices of entities that have been eligible case managers.

19 The IPPs apply to the acts and practices of 'eligible hearing service providers' in connection with the provision of hearing services under an agreement made under Part 3 of the *Hearing Services Administration Act 1997* (Cth): *Privacy Act 1988* (Cth) ss 6(1), 7(1)(cc). An 'eligible hearing service provider' means an entity that is, or has been, engaged under Part 3 of the *Hearing Services Administration Act* to provide hearing services: *Privacy Act 1988* (Cth) s 6(1).

capacity.[20] Other acts and practices of ministers are exempt from the operation of the Act.[21]

37.14 There is no exemption for government ministers from privacy legislation in the United Kingdom, Italy, New Zealand or Hong Kong. In Victoria and Tasmania, privacy legislation provides expressly that it applies to government ministers.[22]

Government inquiries

37.15 In 2000, the Privacy Amendment (Private Sector) Bill was referred to the House of Representatives Standing Committee on Legal and Constitutional Affairs for inquiry and report (2000 House of Representatives Committee inquiry). The 2000 House of Representatives Committee inquiry noted that the political exemption seeks to strike a balance between freedom of political communication and the public interest in protecting the privacy of individuals. The inquiry stated that the exemption seemed to be targeted at the vitality and proper functioning of representative democracy, which requires that parliamentarians be able freely and fully to engage in the democratic process. In the Committee's view, for parliamentarians properly to represent their constituents, they must respond in a more targeted way to their electorates, which requires that they collect and use certain information concerning constituents.[23]

37.16 The 2000 House of Representatives Committee inquiry considered that the drafting of the exemption for political acts and practices needed to indicate clearly that it was intended to support only legitimate purposes, such as serving constituents.[24] It therefore recommended that the exemption be restricted to 'the participation in the parliamentary or electoral process', rather than 'the participation by the political representative in another aspect of the political process'.[25] The Australian Government rejected the recommendation on the basis that this would narrow significantly the scope of the exemption.[26]

37.17 The 2000 House of Representatives Committee inquiry also recommended that a new provision be inserted to provide that the exemption not allow political parties or political representatives to sell or disclose personal information collected in the course

---

20 *Privacy Act 1988* (Cth) s 7(1)(d)–(ed).

21 Ibid s 7(1)(a)(iii).

22 *Information Privacy Act 2000* (Vic) s 9(1)(a); *Personal Information Protection Act 2004* (Tas) s 3 (definition of 'public sector body').

23 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [5.43]–[5.46].

24 Ibid, [5.46].

25 Ibid, recs 11, 12.

26 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

of their duties to anyone not covered by the exemption.[27] The Australian Government rejected this recommendation on the basis that the exemption would operate in a manner that would address the inquiry's concern.[28] A note was inserted in the Bill, however, to make it clear that the exemption does not extend to the use or disclosure (by way of sale or otherwise) of personal information collected by virtue of the exemption in a way that is not covered by the exemption.[29]

37.18 In 2005, the Senate Legal and Constitutional References Committee reviewed the private sector provisions of the *Privacy Act* (Senate Committee privacy inquiry).[30] A number of submissions to the Senate Committee privacy inquiry objected strongly to the exemption for political acts and practices.[31] The Senate Committee privacy inquiry considered the exemption problematic and recommended that the ALRC examine, as part of a wider review of the *Privacy Act*, the operation of, and need for, the exemptions under the *Privacy Act*, particularly in relation to political acts and practices.[32]

International instruments

37.19 The Explanatory Memorandum to the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development states that exceptions to the privacy principles are to be limited to those that are 'necessary in a democratic society'.[33] The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) contains a specific exemption allowing the compilation of data by political parties on people's political opinion in the course of electoral activities, provided that appropriate safeguards are established.[34] Under the EU Directive, the processing of data by political organisations for marketing purposes is also permitted, subject to certain conditions.[35] The Asia-Pacific Economic Cooperation Privacy Framework does not contain a specific exemption or exception concerning political or electoral activities.

---

27 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), rec 13.

28 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

29 Further Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [1]; *Privacy Act 1988* (Cth), note to s 7C.

30 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

31 Ibid, [4.87]–[4.94].

32 Ibid, [7.29]–[7.30], rec 11.

33 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [47].

34 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recital 36.

35 Ibid, recital 30.

37.20 In September 2005, an international conference of privacy and data protection commissioners adopted a *Resolution on the Use of Personal Data for Political Communication*. The Resolution states that any processing of personal data for the purposes of political communication must respect the fundamental rights and freedoms of interested persons and must comply with specific data protection principles. In particular, the Resolution provides that certain principles concerning the collection of personal data, data quality and security, rights of access and correction, and the right to opt out of unsolicited communication should be observed in political communication. In addition, the Resolution recommends that the processing of personal data be based on the individual's consent or another legitimate ground provided for by the law.[36]

Electoral databases

37.21 Electoral databases are databases maintained by political parties that contain information on voters, which may include voters' policy preferences and party identification.[37] It has been argued that the use of such databases raises some common problems, including: political parties withholding from voters information they have stored; inaccurate information being stored on databases without giving voters the right to correct the record; political parties failing to inform voters that information is being compiled about them; and representatives of political parties failing to identify themselves appropriately when collecting information.[38]

37.22 On the other hand, it has been said that electoral databases serve to improve the functioning of representative democracy by: transmitting information more efficiently between members of parliament and a large of number of constituents; allowing early identification of issues important to the electorate; and giving parliamentarians a comprehensive and accurate picture of public opinion in their electorates.[39]

37.23 Proposals for reform in this area include: allowing freedom of information requests in relation to electoral databases; giving voters the option to exclude the local member of parliament from viewing the information on their electoral enrolment forms; prohibiting parliamentarians from forwarding voter information to third parties, including the central party organisation or to support candidates in a different tier of government; better and more uniform training for the database operators, particularly in the ethics of handling personal information; introducing severe penalties for misuse

---

36 *Resolution on the Use of Personal Data for Political Communication (Adopted at the 27th International Conference on Privacy and Personal Data Protection, Montreux, 14–16 September 2005)* (2005) <www.privacyconference2005.org> at 1 August 2007.

37 P van Onselen and W Errington, 'Electoral Databases: Big Brother or Democracy Unbound?' (2004) 29 *Australian Journal of Political Science* 349, 349.

38 P van Onselen and W Errington, 'Suiting Themselves: Major Parties, Electoral Databases and Privacy' (2005) 20 *Australasian Parliamentary Review* 21, 28.

39 P van Onselen and W Errington, 'Electoral Databases: Big Brother or Democracy Unbound?' (2004) 29 *Australian Journal of Political Science* 349, 362–363.

of the database software; and transferring voter information to a central database to which all politicians have access.[40]

Implied freedom of political communication

37.24 Any proposed removal or narrowing of the exemption for political acts and practices needs to be considered in light of the constitutional doctrine of implied freedom of political communication.[41] The High Court of Australia has established that an essential element of representative democracy is the freedom of public discussion of political and economic matters.[42] This freedom is not confined to election periods.[43] It does not, however, confer a personal right on individuals, but rather operates as a restriction on legislative and executive powers.[44] The freedom is not absolute,[45] and must be balanced against other public interests. In determining whether a law infringes the implied freedom of political communication, two questions must be answered:

> First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end …[46]

37.25 One option for ensuring that the coverage of registered political parties and political acts and practices by the *Privacy Act* does not contravene the implied freedom of political communication would be to adopt the model provision contained in the *Parliamentary Counsel's Drafting Direction No 3.1—Constitutional Law Issues*.[47] A provision could be inserted in the *Privacy Act* stating:

> This Act does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.[48]

---

40 P van Onselen and W Errington, 'Political Party Databases: Proposals for Reform' (2004) 6 *Australian Journal of Professional and Applied Ethics* 82.

41 *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1; *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

42 *R v Smithers; Ex parte Benson* (1912) 16 CLR 99, 108, 109–110; *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, 73; *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 177 CLR 106, 232.

43 *Cunliffe v Commonwealth* (1994) 182 CLR 272, 327; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 560–561.

44 *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

45 *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1, 51, 76–77, 94–95; *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 177 CLR 106, 142–144, 159, 169, 217–218; *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 126; *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211, 235; *Cunliffe v Commonwealth* (1994) 182 CLR 272, 336–337, 387; *Langer v Commonwealth* (1996) 186 CLR 302, 333–334; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

46 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567.

47 Australian Government Office of Parliamentary Counsel, *Drafting Direction No 3.1—Constitutional Law Issues* (2006).

48 Ibid, [8].

37.26 Such a provision is currently contained in several pieces of legislation, including the *Spam Act*, the *Do Not Call Register Act*, the *Criminal Code Act 1995* (Cth) and the *Telecommunications Act 1997* (Cth).[49]

Submissions and consultations

Registered political parties

37.27 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether registered political parties should be exempt from the operation of the privacy principles in the *Privacy Act*.[50] There was considerable support for the abolition of the exemption.[51]

37.28 It was suggested in some submissions that preferential treatment of registered political parties—by exempting them from compliance with the *Privacy Act*—undermines public trust in the political process. The Centre for Law and Genetics submitted that 'political parties should act in the public interest and should not be allowed to breach public privacy standards for political ends'.[52] Electronic Frontiers Australia Inc stated that to treat political parties differently from other organisations 'is to send a message that the *Privacy Act* is only a token gesture, to be evaded when it happens to suit particular vested interests with the political clout to get their own way'.[53] Similarly, the Hon Bob Such MP objected to 'political parties being given an exemption to hold personal information for campaigning purposes … a practice not permitted for others'.[54] The Queensland Council for Civil Liberties stated that it failed 'to see how political parties are any different from private companies in their need to be able to respond "in a more targeted way to their electorate"'.[55]

37.29 Some stakeholders accepted that the constitutional doctrine of implied freedom of political communication has some implications in this context, but disputed that this

---

49 *Spam Act 2003* (Cth) s 44; *Do Not Call Register Act 2006* (Cth) s 43; *Criminal Code Act 1995* (Cth) s 102.8(6); *Telecommunications Act 1997* (Cth) s 138. See also *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS(13); *Broadcasting Services Act 1992* (Cth) s 61BG; *Olympic Insignia Protection Act 1987* (Cth) s 73; *Interactive Gambling Act 2001* (Cth) s 61BB(4).

50 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–7.

51 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Confidential, *Submission PR 134,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

52 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

53 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

54 B Such, *Submission PR 71,* 2 January 2007.

55 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

requires a blanket exemption.[56] The Queensland Council for Civil Liberties suggested that the implications of the doctrine would be 'minor'.[57] Professor Graham Greenleaf, Nigel Waters and Associate Professor Lee Bygrave submitted that:

> it is difficult to see why this extends to forcing information onto an individual who has expressed a clear preference not to receive it. There are many alternative means for politicians to communicate with electors. However, the constitutional right should define the ambit of any exemption.[58]

37.30 The New South Wales Council for Civil Liberties Inc submitted that, subject to the constitutional doctrine of implied freedom of political communication, political parties should be bound by the *Privacy Act*. It suggested that, if an exemption were to apply at all, it should only apply 'so far as is necessary for political parties to check electoral rolls during election periods'.[59]

37.31 Stakeholders were also concerned that: political parties can collect information about constituents from third parties that could be inaccurate;[60] and constituents do not know what information was collected by the parties and have no right of access or correction in relation to the electoral databases.[61] A particular concern was that political parties may be able to gather and store information about the ethnicity or religion of electors.[62] For example, one concerned individual claimed that a federal member of parliament had used the electoral roll to identify Jewish members of the electorate through their surnames and send out a newsletter targeting these electors, and the individual had to make repeated requests to have his name removed from the list.[63]

37.32 It was observed that the exemption under the EU Directive for compilation of data by political parties is more limited than the exemption under the *Privacy Act*—for example, the exemption under the EU Directive does not exclude the principles of access or security.[64]

37.33 The Office of the Victorian Privacy Commissioner endorsed the view of the previous Victorian Privacy Commissioner, Paul Chadwick, that the exemption of political parties requires attention. Chadwick was of the view that, although there is a

---

56 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

57 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

58 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

59 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

60 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Confidential, *Submission PR 134,* 19 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

62 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Confidential, *Submission PR 50,* 15 August 2006.

63 Confidential, *Submission PR 50*, 15 August 2006.

64 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

legitimate need for electoral databases for the proper functioning of a democratic community, political parties need to be more open and accountable about these databases in order to promote public trust in the parliament and the political process.[65]

37.34 The OPC noted that it received 'very few complaints or inquiries about the political exemption and therefore the *Privacy Act* may currently provide an appropriate balance'. Nevertheless, the OPC was of the view that if the political exemption is retained, there are two options to enhance privacy protection.[66] One option is to extend s 6EA of the *Privacy Act*, which allows small business operators to voluntarily opt-in to coverage by the Act, to any organisations that are exempt from the operation of the *Privacy Act*, including political parties. Another option is to amend the *Privacy Act* to ensure partial coverage of the political parties by the NPPs. The OPC suggested that:

> consideration be given to requiring political parties to comply with a few key principles, in particular the openness and access and correction principles along with some limits placed on their ability to disclose personal information.[67]

37.35 To date, the ALRC has received no submissions from the federal political parties despite letters from the ALRC specifically inviting a submission on this issue.[68]

Political acts and practices

37.36 In IP 31, the ALRC asked whether political acts and practices should be exempt from the operation of the *Privacy Act*, and if so, whether the current exemption of such acts and practices strike an appropriate balance between the protection of personal information and the implied freedom of political communication.[69] A number of stakeholders expressed support for political acts and practices being exempt only to the extent that it would infringe the constitutional doctrine of implied freedom of political communication.[70]

37.37 The Australian Privacy Foundation and Greenleaf, Waters and Bygrave submitted that a specific exception relating to political acts and practices may be justified only if compliance with any of the privacy principles interferes with the

---

65 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

66 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

67 Ibid.

68 In October 2006, the ALRC wrote to the Liberal Party of Australia, Australian Labor Party, National Party of Australia, Country Liberal Party, Australian Democrats, Australian Greens, and Family First Party.

69 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–8.

70 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; K Handscombe, *Submission PR 89,* 15 January 2007.

operation of representative democracy.[71] Some stakeholders suggested that there is no sound policy reason why the principles of notification, data quality and security, and access and correction do not apply to personal information used in political acts and practices.[72]

37.38 The Centre for Law and Genetics noted 'recent concerns that the staff of elected parliamentarians sometimes go beyond service to their electorate and involve themselves in overtly political promotion and lobbying'.[73] A particular concern raised was that individuals who contacted their local member of parliament or other politicians may have their personal information included in an electoral database. Electronic Frontiers Australia Inc submitted that:

> Such practices have the effect of discouraging some people from participating in the democratic process arising from the knowledge that their personal information will be passed on to third parties and secretly stored potentially forever with no means of finding out whether it is accurate or not.[74]

37.39 One individual cited an example where personal information—including an individual's name and home address—had been disclosed by a member of parliament in parliamentary papers and published on the parliament's website. She submitted that, in addition to the effect of a breach of privacy on an individual, the exemption has a

> general chilling effect on political activism or citizens petitioning politicians for help with personal issues when we know that our correspondence with them may be used or disclosed to third parties in various ways that we cannot control, including … instant publication to the web.[75]

37.40 Concerns have also been raised in relation to the handling of personal health information by members of parliament. The Office of the Health Services Commissioner (Vic) submitted that the exemption should not be retained because 'with the exemption, the possibility exists for politicians to use their political position to breach privacy when handling personal or health information'. The Office stated that the lack of a similar exemption in the *Health Records Act 2001* (Vic) 'has not led to any adverse consequences to the democratic process in Victoria'.[76]

37.41 Similarly, the Royal Women's Hospital Melbourne submitted that the *Privacy Act* should be amended to ensure that politicians are accountable for protecting privacy of personal and sensitive health information. It was particularly concerned that

---

71 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

72 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

73 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

74 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

75 Confidential, *Submission PR 134,* 19 January 2007.

76 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

politicians cannot be investigated by the Privacy Commissioner for breaching patient confidentiality.[77]

37.42 On the other hand, the Hon Bob Such MP suggested that the exemption should extend to the activities of members of parliament when they seek information on behalf of constituents.[78]

Ministers

37.43 The OPC observed that the formulation of the exemption applying to Australian Government ministers is complex:

> In the *Privacy Act* under s 6(1), a Minister is defined as an 'agency' and is therefore covered by the Act, however, his or her acts are excluded from coverage of the *Privacy Act* under s 7(1)(a)(iii). However, a Minister acting in his or her official capacity in relation to agencies within his or her portfolio are covered under ss 7(1)(d), (e), (ea), (eb), (ec), and (ed). … to help reduce this complexity, the definition of 'agency' which currently includes a Minister, should add words that describe the specific acts and practices of the Minister that are covered.[79]

37.44 In addition, it was said that the exemption is difficult to apply. As discussed above, ministers acting in their official capacity are bound by the *Privacy Act*, while members of parliament engaging in political acts and practices are not. The Office of the Victorian Privacy Commissioner submitted that:

> It is sometimes difficult to determine in what capacity a Minister acts—in their Ministerial capacity or in their capacity as an elected Member of Parliament—when personal information is collected and disclosed, at times under the umbrella of Parliamentary immunity. It is also unclear whether Ministerial advisors are subject to privacy obligations, given the nature of their employment and principles of ministerial accountability.[80]

37.45 One individual submitted that the exemption applying to ministers results in 'a danger that the information they hold will be used for political purposes and not for the benefit of the individual or the safety of the nation'.[81]

ALRC's view

37.46 In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. There seems to be no sound policy reason why political parties and those engaging in political acts and practices should

---

77 Royal Women's Hospital Melbourne, *Submission PR 108,* 15 January 2007.
78 B Such, *Submission PR 71,* 2 January 2007.
79 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
80 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
81 K Handscombe, *Submission PR 89,* 15 January 2007.

not be required to handle personal information about individuals in accordance with the *Privacy Act*. For example, there is no justification for political parties and those engaging in political acts and practices to be exempt from: collecting information by lawful and fair means; ensuring the quality and security of the information; setting out their policies on their management of personal information; letting an individual know what personal information is held about the individual; and allowing an individual the right to access and correct such information.

37.47 While the ALRC acknowledges that the OPC has received few complaints or inquiries about the political exemption, significant concerns regarding the electoral databases maintained by political parties and the handling of individuals' sensitive information by members of parliament have been raised in submissions and consultations.

37.48 A number of overseas jurisdictions do not exempt political parties or those engaging in political acts and practices from compliance with privacy legislation, including the United Kingdom, Canada, New Zealand and Hong Kong. Significantly, the *Data Protection Act 1998* (UK) does not contain a political exemption despite the fact that the EU Directive contains a specific exemption allowing, with appropriate safeguards, the compilation of data by political parties on people's political opinions in the course of electoral activities.

37.49 For these reasons, the ALRC considers that registered political parties and political acts and practices should only be exempt to the extent required to avoid a contravention of the implied freedom of political communication. The ALRC is conscious of the fact that the narrowing of the exemption needs to take into account this constitutional doctrine. The ALRC proposes that the model provision in the *Parliamentary Counsel's Drafting Direction No 3.1—Constitutional Law Issues* be adopted to ensure that the *Privacy Act* be read down so that it does not infringe the constitutional doctrine of implied freedom of political communication.

37.50 Whether any act or practice would infringe the doctrine of implied freedom of political communication would be determined on a case-by-case basis by the relevant court or tribunal. In the ALRC's view, it is unlikely that the application of privacy principles to registered political parties and political representatives—including the proposed 'Anonymity and Pseudonymity', 'Specific Notification', 'Openness', 'Data Quality', 'Data Security', 'Access and Correction', 'Identifiers' and 'Transborder Data Flows' principles—would infringe the doctrine.

37.51 The proposed modification of the political exemption under the *Privacy Act* is not intended to displace more specific legislation that permits the collection and use of personal information by registered political parties and political representatives, including the *Commonwealth Electoral Act*, the *Do Not Call Register Act* and the *Spam*

Act.[82] The relevant provisions in these Acts are intended to ensure that freedom of political communication is maintained. The operation of the *Privacy Act* alongside these more specific provisions should ensure that an appropriate balance between the interests of privacy and freedom of political communication is achieved.

37.52 Currently, Australian Government ministers acting in their official capacity are subject to the *Privacy Act*. Given the proposed modification of the political exemption, there seems to be no policy basis for exempting ministers when they are *not* acting in their official capacity, unless they fall within another exemption from the Act.[83] Accordingly, the ALRC also proposes that the partial exemption that applies to Australian Government ministers be removed.

37.53 Before the proposed removal of the political exemption and the exemption applying to Australian Government ministers comes into effect, it would be desirable for the OPC to provide guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act. It is envisaged that the guidance would be directed towards registered political parties and political representatives, their contractors, subcontractors and volunteers.

Proposal 37–1 The *Privacy Act* should be amended to remove the exemption for registered political parties and the exemption for political acts and practices by:

(a) deleting the reference to a 'registered political party' from the definition of 'organisation' in s 6C(1) of the Act;

(b) repealing s 7C of the Act; and

(c) removing the partial exemption that is currently applicable to Australian Government ministers in s 7(1) of the Act.

Proposal 37–2 The *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.

---

82 This is consistent with the ALRC's proposal that the general requirements under the proposed 'Direct Marketing' principle under the proposed Unified Privacy Principles should be displaced to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing, such as the *Do Not Call Register Act* and the *Spam Act*: Ch 23, Proposal 23–2.

83 For example, when they are handling personal information as individuals in the context of their personal, business or household affairs.

Proposal 37–3 Before the proposed removal of the exemptions for registered political parties and for political acts and practices from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act.

38. Media Exemption

Contents

Introduction 1081
- Broadcast media 1082
- Print media 1087
- Journalists 1087
- Complaint statistics 1088
- International instruments 1088
- Overseas jurisdictions 1089

Scope of the exemption 1090
- Background 1090
- Submissions and consultations 1092
- Options for reform 1098
- ALRC's view 1098

Criteria for media privacy standards 1100
- Submissions and consultations 1101
- ALRC's view 1103

Adequacy of the self-regulatory and co-regulatory models 1106
- Overseas jurisdictions 1108
- Submissions and consultations 1108
- ALRC's view 1109

Enforcement mechanisms 1110
- Submissions and consultations 1110
- ALRC's view 1111

Introduction

38.1 Under s 7B(4) of the *Privacy Act 1988* (Cth), acts and practices of a 'media organisation' in the course of journalism are exempt from the operation of the Act if the organisation is publicly committed to observe privacy standards that have been published in writing, either by the organisation, or by a person or body representing a class of media organisations. A 'media organisation' is defined as an organisation (which includes an individual)[1] that collects, prepares or disseminates to the public,

1 An 'organisation' is defined, with certain exceptions, to mean an individual, a body corporate, a partnership, any other unincorporated association or a trust: *Privacy Act 1988* (Cth) s 6C.

news, current affairs, information or documentaries; or commentaries and opinions on, or analyses of, such material.[2]

38.2 The phrase 'in the course of journalism' has not been defined or judicially considered in Australia. When the Privacy Amendment (Private Sector) Bill 2000 (Cth) was first introduced, 'journalism' was defined as the collection, preparation and dissemination of news, current affairs, documentaries and other information to the public.[3] The definition was, however, omitted from the Act 'so that the ordinary meaning of the word will apply'.[4] The term 'journalism' is intended to apply in a technologically neutral way. It is also intended to cover the dissemination of material to the public.[5] The terms 'news', current affairs' and 'documentary' are also not defined.

38.3 Section 66(1A) of the *Privacy Act* provides that a journalist can refuse to give information, answer questions or produce a document or record when so required by the Act if doing so would tend to reveal the journalist's confidential source.[6]

38.4 The reason given for the media exemption was the need to ensure an appropriate balance between the public interest in allowing the free flow of information to the public through the media, and the public interest in safeguarding adequately the handling of information.[7]

38.5 Although there is recognition that an exemption for media activities may be appropriate, some privacy concerns have been raised about the: broad scope of the exemption; lack of criteria and independent assessment of media privacy standards; adequacy of the self-regulatory model; and lack of strong enforcement mechanisms in some media sectors. This chapter discusses these privacy concerns and considers whether any reform of the media exemption is warranted.

Broadcast media

38.6 The broadcast media are regulated by the *Broadcasting Services Act 1992* (Cth), which aims to apply differing levels of regulatory control across a range of broadcasting and other services according to the degree of influence that the various

---

2 Ibid s 6(1).

3 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

4 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [2].

5 Ibid, [4].

6 The ALRC previously recommended that the uniform Evidence Acts be amended to provide for a professional confidential relationship privilege, which includes the privilege between journalists and their sources: Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Recs 15–1, 15–3.

7 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 4, notes on clauses [112]. The right to freedom of expression is recognised in the *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19(2), (3).

media services are able to exert in shaping community views in Australia.[8] The Act requires radio and television industry groups to develop, in consultation with the Australian Communications and Media Authority (ACMA), codes of practice to apply to the broadcasting operations of each section of the broadcasting industry.[9] The codes must take into account any relevant research conducted by ACMA. Industry codes that have been approved by ACMA are included on ACMA's Register of Codes of Practice. ACMA may impose a licence condition requiring the broadcasting licensees to comply with an applicable code of practice.[10] It is an offence to fail to comply with a licence condition. ACMA may also determine program standards to apply to a section of the industry where no codes of practice have been developed or where a code fails to provide appropriate community safeguards.[11]

38.7 ACMA has also developed *Privacy Guidelines for Broadcasters*. These are intended to assist broadcasters and the public to understand better the operation of the privacy provisions in the industry codes. They provide an overview of the way in which ACMA will assess complaints concerning alleged breaches of the privacy provisions.[12]

Private sector broadcasters

38.8 Privacy provisions are included in the codes of practice developed for the following industry sectors: commercial television; commercial radio; subscription broadcast television; subscription narrowcast television; community television; community radio; and open narrowcast radio.[13]

38.9 The coverage of the codes of practice for private sector broadcasters differs as between industry sectors. In the commercial broadcasting sectors, the privacy provisions relate only to news and current affairs programs, whereas in the community broadcasting sectors, the privacy provisions relate to all programs.[14] There are no specific privacy provisions in the codes of practice developed for the open narrowcast television and radio sectors. Some, but not all, codes of practice provide that certain

---

8 *Broadcasting Services Act 1992* (Cth) s 4(1).

9 Ibid s 123.

10 Ibid ss 44(2), 88(2), 92J(2), 100(2), 119(2).

11 Ibid s 125.

12 Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), 1.

13 *Commercial Television Industry Code of Practice* (2004); Commercial Radio Australia, *Codes of Practice & Guidelines* (2004); Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007); Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Television* (2007); Community Broadcasting Association of Australia, *Community Television Code of Practice*; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002); Australian Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007).

14 *Commercial Television Industry Code of Practice* (2004) s 4; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 2; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002), Code 2.

programs must not use material relating to a person's personal or private affairs, or which invades a person's privacy, unless there is a public interest for the materials to be broadcast.[15] Further, licensees should not broadcast the words of an identifiable person unless the person has been informed in advance or his or her consent was obtained before the broadcast.[16] Significantly, only two of the codes of practice address the issue of privacy of children.[17] All of the codes of practice, however, cover the handling of complaints from the public.[18]

National broadcasters

38.10 The Australian Broadcasting Corporation (ABC) is a statutory corporation and Australia's only national, non-commercial broadcaster. The functions of the ABC are to: provide within Australia broadcasting services of a high standard as part of the Australian broadcasting system consisting of national, commercial and community sectors; transmit to countries outside Australia broadcasting programs of news, current affairs, entertainment and cultural enrichment; and encourage and promote the musical, dramatic and other performing arts in Australia.[19]

38.11 The Special Broadcasting Service (SBS) is Australia's multicultural and multilingual public broadcaster. It was established under the *Special Broadcasting Services Act 1991* (Cth) to provide multilingual and multicultural radio and television services.[20]

38.12 Pursuant to s 7(1)(c) of the *Privacy Act*, both the ABC and SBS are covered by the Act except in relation to their program materials and datacasting content.[21]

---

15 *Commercial Television Industry Code of Practice* (2004), s 4; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 2; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007), Code 3; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.

16 *Commercial Television Industry Code of Practice* (2004), Code 4.3; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 6; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.5; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Radio* (2007) Code 1.5; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002), Code 2.5; Australian Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007), Code 1.5. The *SBS Codes of Practice* also contains a similar provision: Special Broadcasting Service, *Special Broadcasting Service, SBS Codes of Practice (2006)*, Code 1.8.

17 *Commercial Television Industry Code of Practice* (2004), Code 4.3; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 3.5.

18 *Commercial Television Industry Code of Practice* (2004), s 7; Commercial Radio Australia, *Codes of Practice & Guidelines* (2004), Code 5; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Broadcast Television* (2007), Code 2; Australian Subscription Television and Radio Association, *Codes of Practice 2007—Subscription Narrowcast Television* (2007), Code 2; Community Broadcasting Association of Australia, *Community Television Code of Practice*, Code 2; Community Broadcasting Association of Australia, *Community Broadcasting Code of Practice* (2002), Code 7; Australian Narrowcast Radio Association, *Codes of Practice Open Narrowcast Radio* (2007), Code 2.

19 *Australian Broadcasting Corporation Act 1983* (Cth) s 6.

20 *Special Broadcasting Service Act 1991* (Cth) s 6.

21 'Datacast' means to broadcast digital information: *Macquarie Dictionary* (online ed, 2005). Under s 6 of the *Broadcasting Services Act 1992* (Cth), 'datacasting service' means a service that delivers content

Section 7A of the Act provides, however, that despite s 7(1)(c), certain acts and practices of the ABC and SBS are to be treated as acts and practices of organisations.[22] Where the acts and practices of the ABC and SBS are to be treated as those of organisations, they may still be exempt if those acts and practices were done in the course of journalism.[23] The specific exemption that applies to the ABC and SBS is discussed further in the context of the public sector in Chapter 33.

38.13 The regulatory regime set out in the *Broadcasting Services Act* for national broadcasting services differs from that for other types of broadcasting services. The ABC and SBS develop their codes of practice through separate consultative processes and are required to inform ACMA of them.[24]

38.14 Privacy provisions are included in the codes of practice for both the ABC and SBS. The *ABC Code of Practice* provides that:

> The rights to privacy of individuals should be respected in all ABC content. However, in order to provide information which relates to a person's performance of public duties or about other matters of public interest, intrusions upon privacy may, in some circumstances, be justified.[25]

38.15 The *SBS Code of Practice* contains a similar provision.[26] In addition, under the *SBS Code of Practice*, SBS is not to transmit the words of an identifiable person except in certain specified circumstances.[27]

Complaints

38.16 Complaints about lack of compliance with a broadcasting code of practice can be made to ACMA only after a written complaint has been made to the particular station, and: the station does not answer the complaint within 60 days; or the complainant is dissatisfied with the station's response.[28] ACMA must investigate such a complaint unless it is satisfied that the complaint is frivolous, vexatious or irrelevant. ACMA has a number of information-gathering powers, including the power to: summon a person to attend before a delegate of ACMA to produce documents or answer questions; examine a person on oath or affirmation; require a person to produce documents for inspection; and hold hearings and direct participants in the hearing to

---

using the broadcasting services bands—whether in the form of text; data; speech, music or other sounds; visual images; or any other form—to persons with the appropriate equipment for receiving that content.

22 There is some ambiguity as to whether those program materials and datacasting content of the ABC and SBS that relate to commercial activities are covered by the private sector provisions of the *Privacy Act*: see discussion in Ch 33.

23 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

24 *Broadcasting Services Act 1992* (Cth) pt 11 div 2; *Australian Broadcasting Corporation Act 1983* (Cth) s 8(1)(e); *Special Broadcasting Service Act 1991* (Cth) s 10(1)(j).

25 Australian Broadcasting Corporation, *ABC Code of Practice* (2004), [2.8].

26 Special Broadcasting Service, *SBS Codes of Practice* (2006), [1.9].

27 Ibid, [1.8].

28 *Broadcasting Services Act 1992* (Cth) ss 148, 150.

attend a conference. Once ACMA has reached a decision, it must notify the complainant of the results of the investigation.[29]

38.17 Where a private sector broadcasting service has breached, or is breaching, a relevant code of practice, ACMA may issue a notice directing a person to take remedial action to ensure compliance.[30] A failure to comply with such a notice is an offence under the *Broadcasting Services Act* and attracts a penalty.[31] In addition, ACMA may impose conditions on licences, including conditions relating to code compliance.[32] In relation to commercial broadcasting, community broadcasting and subscription television services, a breach of a licensing condition could also lead to suspension or cancellation of the broadcasting licence.[33] If ACMA is satisfied that the codes of practice are not providing appropriate community safeguards, it must determine a standard.[34]

38.18 Furthermore, ACMA has been given new enforcement powers based on the findings of a report prepared by Professor Ian Ramsay at the request of the Australian Broadcasting Authority (now ACMA) on the reform of the enforcement powers of the Australian Broadcasting Authority.[35] Under the *Communications Legislation Amendment (Enforcement Powers) Act 2006* (Cth), ACMA is now able to accept enforceable undertakings in relation to compliance with the *Broadcasting Services Act* and registered codes of practice. If ACMA considers that a person has breached such an undertaking, it may apply to the Federal Court of Australia for an order directing compliance with the undertaking, the payment of compensation for another person's loss or damage suffered as a result of the breach, or the payment to ACMA of the amount of any financial benefit the person has obtained that is reasonably attributable to the breach.

38.19 While ACMA does not register the codes of practice under which national broadcasters operate, it has a role in investigating unresolved complaints arising from broadcasts and taking action where the complaint is justified.[36] If a complaint is upheld in relation to a national broadcaster, ACMA may recommend, by written notice, that the national broadcaster take action to comply with the relevant code of practice, or take other action as specified in the notice. Such action may include broadcasting or otherwise publishing an apology or retraction.[37] If the recommendation is not followed

29 Ibid s 149(3), 152(3).
30 Ibid s 141(6).
31 Ibid s 142.
32 Ibid ss 44, 88, 92J, 100, 119.
33 Ibid s 143.
34 Ibid s 125.
35 I Ramsay, *Reform of the Broadcasting Regulator's Enforcement Powers* (2005) Australian Communications and Media Authority.
36 *Broadcasting Services Act 1992* (Cth) pt 11 div 2.
37 Ibid s 152.

within 30 days, ACMA may give the responsible minister a written report on the matter, and the minister must table the report in Parliament.[38]

Print media

38.20 The Australian Press Council (APC) is a self-regulatory body that deals with the print media. Its stated objectives are to help preserve the freedom of the press within Australia and ensure that the press acts responsibly and ethically.[39]

38.21 The APC has published a set of *Privacy Standards* for the purposes of the media exemption under the *Privacy Act*.[40] The *Privacy Standards* deal with the collection, use and disclosure, quality and security of personal information; anonymity of sources; correction, fairness and balance; and the handling of sensitive information. The APC receives and deals with complaints about possible breaches of these Standards, but it will not hear a complaint that is subject to legal action or possible legal action, unless the complainant is willing to sign a waiver of the right to such action.[41] The APC secretariat will try to negotiate the settlement of a complaint, failing which a formal response will be sought from the publication and sent to the complainant. If the complainant is not satisfied with the response, he or she, with the agreement of the newspaper, can seek a conciliation hearing conducted by the APC, or can immediately refer the matter to the APC for adjudication. If asked to adjudicate, the APC's Complaints Committee holds a hearing and makes a recommendation to the APC. The APC has no power to penalise or make an order against a publication; it can only distribute the Committee's findings to the media and publish them in the APC's newsletters and annual reports.[42]

Journalists

38.22 The Media Entertainment and Arts Alliance is the union and professional organisation for the media, entertainment, sports and arts industries.[43] Journalist members of the Alliance are bound by its *Code of Ethics*. The *Code of Ethics* provides for certain privacy standards, including the requirement that journalists: do not place unnecessary emphasis on personal characteristics such as race, ethnicity and religious beliefs; identify themselves and their employer before obtaining an interview; and respect private grief and personal privacy.[44]

---

38 Ibid s 153.

39 Australian Press Council, *About the Council* <www.presscouncil.org.au/pcsite/apc.html> at 14 August 2007.

40 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 30 July 2007.

41 Australian Press Council, *How to Make a Complaint: An Overview* <www.presscouncil.org.au/pcsite/complain.html> at 14 August 2007.

42 Ibid.

43 Media Entertainment and Arts Alliance, *Alliance Online* <www.alliance.org.au> at 14 August 2007.

44 Media Entertainment and Arts Alliance, *Media Alliance Code of Ethics* <www.alliance.org.au/code-of-ethics.html> at 14 August 2007, [2], [8], [11].

38.23 Where a person believes that a journalist member of the Alliance has breached the Code, he or she may make a formal complaint to the Alliance. If the Alliance finds the complaint proven, it can censure or rebuke the journalist, fine the journalist up to $1,000 for each offence, or expel the journalist from membership of the Alliance. Information about complaints against journalists is published and distributed on an annual basis to journalist members of the Alliance.[45]

Complaint statistics

38.24 The Office of the Privacy Commissioner (OPC) examined the media exemption as part of its review of the private sector provisions of the *Privacy Act* (OPC Review). The OPC noted that it had received very few inquiries and complaints about media organisations.[46] During the period between 21 December 2001 and 31 January 2005, the OPC indicated that 1% of all the NPP complaints closed by the OPC on the basis that they were outside of its jurisdiction concerned the media exemption.[47]

38.25 From July 1996 to June 2006, the Australian Broadcasting Authority, and subsequently ACMA, has conducted a total of 82 privacy related investigations involving commercial television; 23 of which were found to involve breaches. For commercial radio, there have been 16 investigations, seven of which involved breaches. During that period, there were no privacy related investigations conducted in relation to the national broadcasters, 1 in relation to the subscription television sector, and 1 in the community broadcasting sector. Neither of these investigations resulted in a finding of breach.[48]

38.26 According to the APC, annually since 2001 there have been 22–25 complaints to the APC on privacy matters.[49]

International instruments

38.27 The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) issued by the Organisation for Economic Co-operation and Development do not specifically provide for an exemption or exception relating to journalistic activities or freedom of expression.[50] The OECD Guidelines recognise, however, that there may be exceptions to the privacy principles, which should be 'limited to those which are necessary in a democratic society'.[51]

---

45 Alliance Online, *Code of Ethics Breaches: How to Complain* <www.alliance.org.au/media/ethics_breach.htm> at 14 August 2007.

46 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 197.

47 Ibid, 328.

48 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

49 Australian Press Council, *Submission PR 48,* 8 August 2006.

50 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

51 Ibid, Guideline 4; Memorandum, [47]. The right to freedom of expression is guaranteed under numerous international human rights instruments, including the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*: *United Nations Universal Declaration of Human*

38.28 The *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) issued by the European Parliament contains a specific exception to the principles for the purposes of journalism, or literary or artistic expression. Article 9 of the EU Directive sets out that Member States shall provide for exemptions or derogations from certain provisions of the EU Directive

> for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[52]

38.29 There are no definitions of 'journalistic purposes', or 'literary or artistic expression' in the EU Directive, and to date, the matter has not come before the European Court of Human Rights. The term 'journalistic purposes' has been considered, however, by the Supreme Court of Sweden.

38.30 In *Case B 293–00*, the Supreme Court of Sweden held that the exemption for 'journalistic purposes' in art 9 of the EU Directive and s 7 of the Swedish *Personal Data Act 1988* applies to a private individual who created a website that published derogatory statements about Swedish banks and named individual employees. The Court declined to limit the meaning of 'journalistic purposes' by reference to the standards of the traditional news media. Instead, the Court focused on identifying the character of the activity taking place. To that end, it suggested that one purpose of journalism was to inform, exercise criticism and initiate debate in societal issues of importance for the public. In addition, the Court held that insulting or derogatory statements in the media could have the character of a journalistic purpose, as they are within the scope of critical societal debate. The Court observed, however, that although the defendant was able to rely on the media exemption in the *Personal Data Act*, he was not immune from other causes of action, including defamation.[53]

Overseas jurisdictions

38.31 Privacy legislation in some overseas jurisdictions provides for an exemption or exception relating to journalistic materials or news activities.[54] In Canada, the personal information protection principles do not apply to personal information collected, used

---

Rights, GA Res 217A(III), UN Doc A/Res/810 (1948) art 19; *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19.

52 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 9. See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), Recitals 17, 37.

53 L Bygrave, 'Balancing Data Protection and Freedom of Expression in the Context of Website Publishing—Recent Swedish Case Law' (2001) 8 *Privacy Law & Policy Reporter* 83.

54 See, eg, *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 4(2)(c), 7(1)(c); *Data Protection Act 1998* (UK) s 32; *Privacy Act 1993* (NZ) s 2(1); *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

or disclosed by a private sector organisation for journalistic, artistic or literary purposes.[55]

38.32 In the United Kingdom, except in relation to data security, the data protection principles do not apply to the processing of personal data for journalistic, artistic or literary purposes (the 'special purposes') where:

> (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
>
> (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
>
> (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.[56]

38.33 Under the *Privacy Act 1993* (NZ), news media are exempt in relation to their news activities.[57] In Hong Kong, businesses that carry on news activities are exempt from compliance with some of the data protection principles in relation to personal data held solely for the purpose of news activity or a directly related activity. Such businesses are exempt from the 'access' principle, 'unless and until the data are published or broadcast'; and the 'use and disclosure' principle, where the data are disclosed by a person who has reasonable grounds to believe, and reasonably believes, that the publishing or broadcasting of the data is in the public interest.[58]

Scope of the exemption

Background

38.34 Does the media exemption strike an appropriate balance between the free flow of information to the public and privacy protection? Some commentators have argued that the exemption is too broad.[59] In 1979, a majority of the ALRC recommended that

---

55 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 4(2)(c), 7(1)(c).

56 *Data Protection Act 1998* (UK) s 32(1). Under the *Data Protection Act 1998* (UK), the seventh data protection principle provides that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data': *Data Protection Act 1998* (UK) sch 1, principle 7.

57 *Privacy Act 1993* (NZ) s 2(1). 'News activity' means: (a) the gathering of news, or the preparation or compiling of articles or programmes concerning news, observation on news, or current affairs, for the purposes of dissemination to the public; or (b) the dissemination of articles or programmes concerning news, observation on news or current affairs to the public: *Privacy Act 1993* (NZ) s 2(1). 'News medium' means 'any agency whose business, or part of whose business, consists of a news activity; but, in relation to principles 6 and 7, does not include Radio New Zealand Limited or Television New Zealand Limited': *Privacy Act 1993* (NZ) s 2(1).

58 *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

59 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13; N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149; N Waters, 'Commonwealth Wheels Turn Again—A Cautious Welcome' (1999) 5 *Privacy Law & Policy Reporter* 127, 128. A similar view was expressed in submissions to the OPC Review: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 196–197.

legislation should provide privacy protection against publication, without reasonable justification, of sensitive private facts relating to an individual, in circumstances where the publication is likely to cause distress, annoyance or embarrassment on an objective view of the position of the individual. The ALRC considered sensitive private facts to be matters relating to the health, private behaviour, home life, or personal or family relationships of an individual.[60]

38.35 It has also been suggested that media reporting of health information runs a high risk of causing harm to individuals and therefore should be subject to tighter regulation.[61]

Definitions

38.36 Another factor that affects the scope of the media exemption is the definition, or lack of definition, of the terms used in the exemption. Particular concerns have been raised in previous inquiries about the lack of definition of the term 'journalism', and the wide definition of the term 'media organisation', in the exemption.[62]

38.37 Originally, the word 'journalism' was defined in the Privacy Amendment (Private Sector) Bill. After the release of the report on the Bill by the House of Representatives Standing Committee on Legal and Constitutional Affairs (2000 House of Representatives Committee inquiry),[63] the Australian Government amended the Bill to omit the definition of 'journalism'.[64] In response to questions by the Senate Legal and Constitutional Legislation Committee inquiry into the Bill, [65] the Attorney-General's Department (AGD) stated that the Australian Government was aware that journalism may change in nature, and that the Supplementary Explanatory Memorandum to the Bill conveyed the Government's intention that the media exemption cover a range of activities of different forms of media.[66]

38.38 The OPC Review recommended the term 'in the course of journalism' be defined and that the term 'media organisation' be clarified in order to ensure that the

---

60 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [236].

61 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 195–196.

62 Ibid, 195–199; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 72–74.

63 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000).

64 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [2]–[4].

65 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000).

66 Ibid, [3.29].

exemption focuses on news and current affairs.[67] The Australian Government disagreed with this recommendation.[68]

38.39 One commentator argued that:

> the everyday meaning of 'journalism' would appear to include entertainment, infotainment and educational output of the media. Arguably, important issues of freedom of speech and the public interest role of the media are confined to news and current affairs.[69]

38.40 In New Zealand, the exemption is confined to a 'news medium' that carries on the business of 'news activities'.[70] 'News medium' means 'any agency whose business, or part of whose business, consists of a news activity'.[71] 'News activity' is defined as:

> (a) The gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:
>
> (b) The dissemination, to the public or any section of the public, of any article or programme of or concerning—
>
> (i) News;
>
> (ii) Observations on news;
>
> (iii) Current affairs:[72]

38.41 In addition, it has been argued that, due to the lack of statutory definitions of the terms 'news', 'current affairs' and 'documentary', the media exemption may apply to any organisation that publishes material, provided that it is publicly committed to observe published media specific privacy standards.[73] This could include any organisation that collects and disseminates personal information over the internet.[74]

Submissions and consultations

38.42 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the acts and practices of media organisations in the course of journalism should be exempt

---

67 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 198, recs 58, 59.

68 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 11.

69 C Vietri, 'The Media Exemption under Information Privacy Legislation: In the Public Interest?' (2003) 8 *Media and Arts Law Review* 191.

70 *Privacy Act 1993* (NZ) s 2(1).

71 Ibid s 2(1).

72 Ibid s 2(1). There is a similar provision in Hong Kong law: *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

73 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149. See also N Waters, 'Commonwealth Wheels Turn Again—A Cautious Welcome' (1999) 5 *Privacy Law & Policy Reporter* 127, 128.

74 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

from the operation of the *Privacy Act* and, if so, what the scope of the exemption should be. The ALRC also asked whether s 7B(4) of the *Privacy Act* strikes an appropriate balance between the free flow of information to the public and the protection of personal information.[75]

38.43 Media organisations and their representative bodies strongly supported retaining the current scope of the media exemption.[76] They submitted that the exemption is working well and strikes an appropriate balance between the flow of information on matters of public concern and individual privacy.[77] The ABC stated that 'the importance of allowing the free flow of information to the public through the media appears to be generally accepted'.[78]

38.44 The Queensland Council for Civil Liberties was also in favour of maintaining the media exemption. It submitted that:

> Freedom of Speech is a fundamental value of our society. It seems to us that all the models for limiting or eliminating press exemption involve creating a system of government regulation of the press which would have an undesirable potential.[79]

38.45 Some stakeholders submitted that the current regulatory framework already provides adequate protection of personal privacy,[80] including a range of federal and state laws and industry codes of practice.[81] The ABC suggested that, since the exemption is only available to media organisations that have committed publicly to published privacy standards, individuals have the means to address privacy concerns arising from the activities of media organisations.[82]

38.46 The APC stated that complaints about media intrusion form 'a very small part' of those received by the OPC and the NSW Privacy Commissioner.[83] ACMA observed that the relatively low number of privacy related investigations and findings of breach suggests that 'the electronic media are acting effectively in balancing privacy issues'. It submitted, however, that an assessment of community concern should not be based solely on the frequency of complaints. The following reasons were given:

---

75 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–10.

76 Free TV Australia, *Submission PR 149,* 29 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007; Australian Press Council, *Submission PR 48,* 8 August 2006.

77 Free TV Australia, *Submission PR 149,* 29 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007; Australian Press Council, *Submission PR 48,* 8 August 2006.

78 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

79 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

80 Free TV Australia, *Submission PR 149,* 29 January 2007; SBS, *Submission PR 112,* 15 January 2007.

81 Free TV Australia, *Submission PR 149,* 29 January 2007.

82 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

83 Australian Press Council, *Submission PR 83,* 12 January 2007; Australian Press Council, *Submission PR 48,* 8 August 2006.

> - ACMA only considers complaints if they have not been satisfactorily resolved by broadcasters. ACMA does not have access to all complaints made directly to broadcasters and so may underestimate community concern in this area;
> - the bringing of complaints of invasion of privacy in effect repeats the invasion. A potential complainant may decide that to proceed with a complaint about an invasion of privacy compounds the problem; and
> - a lower level of complaints about invasion of privacy is to be expected, because individuals who are not directly affected are less likely to complain. In contrast, areas such as bias or inaccuracy generate complaints from members of the public generally.[84]

38.47 In its submission to the OPC review, the Australian Privacy Foundation suggested that the low level of complaints and inquiries does not indicate satisfaction with the exemption, but rather 'a widespread and correct view that the media are effectively above the law in relation to privacy'.[85]

38.48 SBS suggested that limiting or removing the media exemption 'risks being a disproportionate response to concerns about abuse of privacy', and that 'any reform … would require a significant social imperative to outweigh the public interest in media freedom'.[86] The ABC observed that the exemption is not unconditional, and suggested that it 'may prove to be too narrow, if the undefined term "journalism" is given a restrictive meaning in future judicial determinations'.[87]

38.49 Some stakeholders considered the scope of the media exemption to be problematic.[88] Electronic Frontiers Australia submitted that the scope of the exemption has become 'seriously problematic' following the introduction of uniform defamation laws, under which truth alone is a defence. It suggested that:

> due in part to the increasing number of individuals who publish 'news' and 'commentary' on the Internet, who may or may not be 'journalists' … we consider individuals should have a cause of action for breach of privacy.[89]

---

84 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

85 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

86 SBS, *Submission PR 112,* 15 January 2007.

87 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

88 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

89 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

38.50 It was suggested in one submission that issues about the balance between privacy rights and freedom of expression should be addressed by selective exceptions to some of the privacy principles, rather than an exemption.[90]

Children and young people

38.51 Some stakeholders raised concerns about the publication by media organisations of children's personal information—including publication that may contravene laws preventing identification of children as witnesses or parties in legal cases.[91] Both the NSW Commissioner for Children and Young People and the Legal Aid Commission of New South Wales were concerned about a number of instances where children allegedly involved in criminal cases have been named or identified publicly by the media.[92] The NSW Commissioner for Children and Young People submitted that 'exempting the acts and practices of media organisations in section 7B(4) of the *Privacy Act* does not adequately protect the privacy of children and young people'.[93]

38.52 The Queensland Government Commissioner for Children and Young People and Child Guardian considered that the current system of voluntary regulation in the reporting of children and young people lacks sufficient safeguards, and it is currently developing guidelines to promote responsible portrayal of children in the media.[94]

> It is important to consider that members of the media might not have education or expertise in assessing whether a child or young person has the capacity to make decisions or exercise rights regarding their personal information. For example, a journalist may mention the name, age and location of a child or young person in an article which may result in that child or young person being identified by a predator or an abusive parent.[95]

38.53 The APC stated that 'whether the individual is a child and warrants a greater level of privacy protection' is one of the factors that is taken into account when it deals with questions of privacy.[96]

Sensitive information

38.54 Another concern raised is the publication of sensitive personal information by journalists. The Centre for Law and Genetics submitted that the media exemption should be limited to the use of non-sensitive personal information, and that:

---

90 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

91 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

92 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

93 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

94 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

95 Ibid.

96 Australian Press Council, *Submission PR 48,* 8 August 2006.

> the use of sensitive personal information could be governed by the NPPs, perhaps with the inclusion of a provision allowing publication where there is reasonable justification.[97]

38.55 The APC stated that its own regime 'recognises the existence of "sensitive private facts" and seeks to ensure that publications do not intrude on them'.[98] The ABC submitted that removing the media exemption and substituting it with a defence of 'reasonable justification' would prove unworkable if the term 'reasonable' is interpreted restrictively.[99]

Definitions

38.56 In IP 31, the ALRC asked whether the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' should be defined in the *Privacy Act*, and if so, how they should be defined.[100] Some stakeholders considered the lack of definitions of these terms problematic.[101] It was submitted that the lack of definition of the term 'journalism', together with the wide definition of the term 'media organisation', 'effectively allows anyone to claim the exemption by setting up a "publishing enterprise"'.[102] In addition, they suggested that:

> If there are to be selective exceptions for public interest media activity, these terms will need to be much more carefully and closely defined. While difficult, it must be possible to distinguish between genuine news and current affairs journalism which deserve some exemption, and the infotainment, entertainment and advertising which makes up the bulk of media content and which should be subject to privacy principles to the maximum extent practicable.[103]

38.57 The Legal Aid Commission of New South Wales submitted that lack of clear definitions of the terms in the exemption is likely to become more problematic,

> given the way that forms of communication such as Internet 'blogs' have come to blur the distinction between commercial media organisations and other people and organizations seeking publicity.[104]

---

97 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
98 Australian Press Council, *Submission PR 83,* 12 January 2007.
99 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.
100 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–11. The ALRC also asked whether there are other terms that would be more appropriate. There was no response to this question in submissions.
101 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
102 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
103 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
104 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

38.58 The Centre for Law and Genetics suggested revisiting the definition of 'journalism' that was originally included in the Privacy Amendment (Private Sector) Bill.[105]

38.59 Other stakeholders were of the view that defining these terms would be impractical given rapidly evolving technology and the changing nature of journalism.[106] The APC submitted that it would not have difficulty with the inclusion of definitions of the terms. It queried, however, whether adequate definitions could be crafted, and suggested that 'there is no evidence that the *Act* suffers from this lack of specific definition'.[107] SBS suggested that the most useful approach is to rely on the ordinary natural meaning of the terms.[108]

38.60 The Victorian Society for Computers and Law submitted that the meaning of the terms used in the media exemption should be established by case law, because any definitions may become obsolete as notions such as 'journalism' and 'news' develop over time. It suggested that, if definitions of those terms were to be included in the *Privacy Act*, they should be: 'technology and media neutral in order to maintain their relevance for any significant period of time'; and 'consistent with the fair dealing exceptions relating to the use of copyright material, including under section 42 of the *Copyright Act 1968* (Cth) for the purpose of reporting the news'.[109]

38.61 The ABC suggested that the terms news, current affairs and documentary 'are terms of wide compass whose meanings may further evolve, and accordingly should not be defined'.[110]

38.62 In response to the question of whether the term 'media organisation' is too wide, the APC stated that it had been 'at pains to ensure that only organisations that are principally publishers of print media can subscribe to the [APC's *Privacy*] *Standards*', rather than others who might, incidentally, publish periodicals.[111] The ABC submitted that the definition of 'media organisation' should be extended:

> Given that the policy reason for the media exemption is to facilitate the free flow of information to the public, the ABC does not see why the exemption should focus narrowly on news and current affairs. Many other media publications may be in the public interest, including documentaries and other information programs.[112]

---

105 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
106 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.
107 Australian Press Council, *Submission PR 83,* 12 January 2007.
108 SBS, *Submission PR 112,* 15 January 2007.
109 Victorian Society for Computers and the Law Inc, *Submission PR 137,* 22 January 2007.
110 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.
111 Australian Press Council, *Submission PR 83,* 12 January 2007.
112 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

Options for reform

38.63 One means of limiting the scope of the media exemption is to require publication of personal information to be in the public interest.[113] Another way to restrict the scope of the exemption is to define some of the terms that are used in the media exemption. In particular, defining the word 'journalism' in s 7B(4) of the *Privacy Act* would have a significant impact on the scope of the exemption. Although 'journalism' is not defined in other federal, state or territory legislation, privacy legislation in comparable jurisdictions or Australian case law, there are a number of other sources on which the word 'journalism' used in the media exemption may be modelled.

38.64 There are four main options for defining the word 'journalism':

- The *Macquarie Dictionary* defines 'journalism' as 'the occupation of writing for, editing, and producing newspapers and other periodicals, and television and radio shows', or 'such productions viewed collectively'.[114]

- The Privacy Amendment (Private Sector) Bill originally defined 'journalism' as 'the collection, preparation and dissemination of news, current affairs, documentaries and other information to the public', including commentary and opinion on, or analysis of, this kind of material.[115] Due to the inclusion of the word 'information', media content such as infotainment, entertainment and advertising may fall within this definition of journalism.

- The definition of 'journalism' originally used in the Privacy Amendment (Private Sector) Bill could be modified by omitting the word 'information'. This would ensure that the exemption is only available in relation to news, current affairs and documentaries.

- As noted above, the *Privacy Act 1993* (NZ) contains a definition of 'news activity' that focuses on news, observations on news and current affairs, and does not include 'documentary' or 'information'.

ALRC's view

38.65 The free flow of information to the public through the media is an important element of a democratic society. This principle is not, however, absolute. It is necessary to balance the free flow of information to the public through the media and the public interest in adequately safeguarding the handling of personal information. Stakeholders recognised the need to reach such a balance. In the ALRC's view, the most appropriate means of reconciling these sometimes competing principles is to

---

113 See, eg, *Data Protection Act 1998* (UK) s 32.

114 *Macquarie Dictionary* (online ed, 2005).

115 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

grant media organisations a limited exemption from the operation of the *Privacy Act*. That is, media organisations should be exempt from complying with the *Privacy Act* when acting in the course of journalism.

38.66 It was suggested that the lack of a statutory definition of 'journalism' allows the exemption to be interpreted too broadly. Consistent with the views of a number of stakeholders, the media exemption should focus primarily on reporting by the media of matters of public interest. It should not exclude from the operation of the Act content such as infotainment, entertainment and advertising. Therefore, the ALRC proposes a modified version of the definition of 'journalism' that was originally included in the Privacy Amendment (Private Sector) Bill, by excluding the word 'information' from that definition. This means that to the extent that media organisations publish material that falls within the ambit of the general word *information*—but is not news, current affairs or documentaries—they will be covered by the *Privacy Act*.

38.67 The ALRC's view is that this proposed definition is preferable to both of the alternative definitions discussed above. First, the *Macquarie Dictionary* of 'journalism' is problematic because it is too broad and it is directed, not to the *content* in question, but to the entities that publish this content. That is, the dictionary definition refers to the media—'newspapers and other periodicals, and television and radio shows'—in which the information appears without mentioning the nature of the information covered. Secondly, the definition of 'news activity' in the *Privacy Act 1993* (NZ) is too narrow because it focuses only on news, observations on news, and current affairs, but does not include documentaries.

38.68 Given that 'news', 'current affairs' and 'documentary' are terms of wide import, the ALRC considers that defining these terms in the *Privacy Act* would be impracticable. Instead, the ordinary meaning of these terms should continue to apply.

38.69 In the ALRC's view, the definition of 'media organisation' should remain as it currently stands. As a result, an individual, for example, will continue to fall within this definition provided he or she can satisfy the relevant criteria in the Act. The ALRC believes that this is an appropriate outcome, because the exemption is designed to protect a type of freedom of expression—that is, expression by media organisations—which has a number of significant public benefits.[116] As Professor David Feldman has explained, one such benefit is that, 'as a tool of self-expression it is a significant instrument of personal autonomy'.[117] As such, it is important that the media exemption not be limited to established media businesses or professional journalists.

38.70 In Chapter 5, the ALRC proposes that the *Privacy Act* be amended to provide for a statutory cause of action for invasion of privacy. The retention of the media

116 See, eg, D Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd ed, 2002), ch 14.
117 Ibid, 802.

exemption is not intended to preclude the proposed statutory cause of action for invasion of privacy from being brought against a media organisation or an individual. It is important to emphasise that, where the media exemption applies, it means that a media organisation is not obliged to comply with the privacy principles. This does not mean, however, that the media organisation would be immune from having an action brought against it under the proposed cause of action. That is a separate question and, if an individual is able to establish that the media organisation is liable under the statutory cause of action, he or she could seek a remedy provided for in the relevant provisions of the Act.

Proposal 38–1 The *Privacy Act* should be amended to define 'journalism' to mean the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs or a documentary; or

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary.

Criteria for media privacy standards

38.71 The *Privacy Act* has been criticised for its lack of criteria for, or independent assessment of, the adequacy of media privacy standards.[118] As noted above, under s 7B(4) of the *Privacy Act*, acts and practices of a 'media organisation' in the course of journalism are exempt from the operation of the Act if the organisation is publicly committed to observe 'standards that deal with privacy in the context of the activities of a media organisation'. The OPC Review stated that it is uncertain whether the Privacy Commissioner has powers under the *Privacy Act* to determine whether those standards provide adequate protection. It suggested that one way to resolve this issue would be to amend s 7B(4) to establish criteria by which the Privacy Commissioner could determine whether the standards are adequate.[119]

38.72 The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to require that the Australian Broadcasting Authority (now ACMA) and media bodies consult with the Privacy Commissioner when developing privacy codes.[120] It also recommended that the OPC, together with ACMA, provide

118 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149. See also T Dixon, 'Communications Law Centre Wants IPPs Revised in Line with Australian Privacy Charter: Extracts from the CLC Submission on the Discussion Paper' (1997) 3 *Privacy Law & Policy Reporter* 171, 172.

119 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 198.

120 Ibid, rec 58.

greater guidance to media organisations on appropriate levels of privacy protection, especially concerning health information, and raise the awareness of organisations that the media exemption is not a blanket exemption.[121]

38.73 The Australian Government did not agree that ACMA and media bodies should be required to consult with the Privacy Commissioner when developing privacy codes. Instead, it was of the view that it would be more appropriate for the OPC to provide guidance and alert organisations to the fact that the media exemption is not a blanket exemption.[122]

Submissions and consultations

38.74 Some stakeholders expressed concern about the inadequacy of the media privacy standards.[123] It was noted in one submission that 'at least some of the current media privacy standards are substantively weak', and that the APC's *Privacy Standards* 'do not contain an equivalent of NPPs 5 (openness) or 9 (transborder data flow) and are more lax in several respects than some of the other NPPs'.[124]

38.75 A concern was raised about the lack of scrutiny of the adequacy of privacy standards.[125] The Centre for Law and Genetics observed that there are significant differences in the way that journalistic acts are regulated across different media. It stated that:

> Currently journalistic acts relating to use of personal information are inadequately regulated in some sectors, largely due to the lack of scrutiny of the adequacy of privacy standards and lack of enforceability of standards.[126]

38.76 Particular concerns were also raised that media privacy standards do not address adequately the privacy needs of children and young people. The Queensland Government Commissioner for Children and Young People and Child Guardian submitted that privacy standards applied through media regulatory bodies do not sufficiently consider the privacy of children and young people and are not regularly enforced.[127] The NSW Commissioner for Children and Young People submitted that the *Privacy Act* should be amended 'to include a provision that requires broadcasters to

---

121 Ibid, rec 59.

122 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), 11.

123 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

124 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

125 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

126 Ibid; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

127 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

include a standard within the industry standard and principles that relates specifically to children and young people'. In addition, it suggested that:

> any standards or principles should recognise that if a parent refuses consent a broadcaster cannot over-ride this consent. However, where a parent does consent, the broadcaster should be subject to a further test of the best interests of the child.[128]

38.77 There was also concern expressed in some submissions about the concept of 'public commitment' to observe privacy standards.[129] It was submitted that 'the condition requiring a public commitment to privacy standards can be satisfied by the organisation itself, with no independent assessment'.[130] The Centre for Law and Genetics stated that the notion of 'public commitment to observe published standards' needs to be clarified.[131]

38.78 A range of reform options were suggested, including: imposing a binding code on media organisations;[132] incorporating media privacy standards into the *Privacy Act*;[133] empowering the OPC to determine the adequacy of media privacy standards;[134] and providing greater guidance to media organisations.[135] The NSW Commissioner for Children and Young People supported a binding code for all broadcasting services,[136] however, the Electronic Frontiers Australia submitted that:

> We are very dubious about proposals to require journalists to subscribe to a binding code etc due to the potential, now or in the future, for such a requirement to restrict 'competition' by requiring journalists, including independent journalists who publish on the Internet without charging fees for access, to pay membership fees (in part to cover code adjudication costs) in order to be able to subscribe to a code.[137]

38.79 The Centre for Law and Genetics submitted that the OPC should be empowered to

> determine whether standards are adequate and particularly whether they provide for sufficient sanctions against non-compliance. In situations where there are no standards, or where the standards are inadequate, the Privacy Commissioner should be given the power to direct that the Act must be complied with.[138]

---

128 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
129 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
130 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
131 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
132 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
133 Confidential, *Submission PR 132,* 18 January 2007.
134 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
135 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.
136 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
137 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
138 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

38.80 Some stakeholders supported the recommendation in the OPC Review that the OPC, in conjunction with ACMA, provide greater guidance to media organisations as to appropriate levels of privacy protection and raise the awareness of organisations that the media exemption is not a blanket exemption.[139]

38.81 Free TV Australia submitted that Australian media are already subject to legislation that adequately protects 'against inappropriate or unfair means of gathering or disclosing information and images'.[140] It noted that there are already privacy requirements in place for broadcasters through the industry codes of practice that are 'specifically adapted to addressing issues of privacy in the media context', and that journalists are subject to privacy requirements through the Journalist's *Code of Ethics*. It stated that, in particular, the codes of practice for the broadcast media are subject to public consultation and review, as well as approval by ACMA.[141]

38.82 The APC stated that it had sought the views of the OPC when developing its *Privacy Standards* for the print media.

> The OPC had adequate opportunity to comment on the Standards while they were in draft form and to contribute to their development. The Council took the OPC's silence to be informed consent.[142]

38.83 The APC stated that all major newspaper publishers, a large number of country newspapers, all major suburban newspapers and a number of magazine publishers have publicly subscribed to the APC's *Privacy Standards*.[143] Furthermore, there have been continuing consultations with publishers and seminars that enable the APC to match its interpretation of the *Privacy Standards* with contemporary community standards.[144] The APC further submitted that there is insufficient evidence that the standards have failed to address public concern about improper handling of information.[145]

ALRC's view

38.84 The current privacy standards of different representative media bodies have varying levels of privacy requirements and some are lacking in detail. In addition, there are no criteria for assessing whether media privacy standards are adequate, and there is no requirement that the OPC be consulted in the development of industry codes of practice or other media privacy standards.

---

139 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.
140 Free TV Australia, *Submission PR 149,* 29 January 2007.
141 Ibid.
142 Australian Press Council, *Submission PR 83,* 12 January 2007.
143 Australian Press Council, *Submission PR 48,* 8 August 2006.
144 Ibid.
145 Australian Press Council, *Submission PR 83,* 12 January 2007.

38.85 One option for reform is for media privacy standards to be incorporated into the *Privacy Act*. The ALRC does not consider that this approach is practical, as privacy standards may need to be adjusted from time to time in light of developing technology. A better alternative is for the OPC to establish criteria for assessing the adequacy of media privacy standards. The criteria should be established in consultation with ACMA and peak media representative bodies, including the APC and the Media Entertainment and Arts Alliance. Once the criteria are established, they should be published by the OPC in the form of guidelines.

38.86 Currently, the terms of the media exemption are silent on the adequacy of media privacy standards. Section 7B(4)(b) of the *Privacy Act* provides that a media organisation is exempt if it was engaging in an act or practice in the course of journalism

> at a time when the organisation is publicly committed to observe standards that:
>
> (i) deal with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters); and
>
> (ii) have been published in writing by the organisation or a person or body representing a class of media organisations.

38.87 In the OPC Review, the OPC stated that:

> It is not clear if this section enables the Commissioner to decide whether or not the standard deals with privacy in an adequate way in the course of establishing whether or not a media organisation is publicly committed to a standard.[146]

38.88 The ALRC considers that the insertion of the word 'adequately' in s 7B(4)(b) will address this concern.

38.89 These proposals do not envisage that the Privacy Commissioner would be required to assess media privacy standards developed by a media organisation in the absence of a complaint. It does, however, mean that if a complaint is made to the Privacy Commissioner about the activities of a media organisation, the Privacy Commissioner would be able to determine whether the media privacy standards were adequate and therefore whether the media exemption applies in that instance. Where the privacy standards are considered adequate, any complaints would be made to the media organisations and the media bodies that oversee the privacy standards. Where the privacy standards are considered 'inadequate', for example, by the Privacy Commissioner, the media exemption would not apply and the Privacy Commissioner would have jurisdiction to deal with the complaint.

38.90 Particular concerns have been raised in submissions about the publication of information and portrayal of children and young people in the media. In Chapter 60, the ALRC proposes that the criteria for assessing the adequacy of media privacy

---

146 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 198.

standards should include specific provisions dealing with the privacy of children and young people.[147]

38.91 The term 'publicly committed' in the media exemption is not defined and has not been the subject of judicial interpretation. Therefore, the ALRC proposes that the OPC clarifies that in order for the media exemption to apply, public commitment by media organisations to observe privacy standards not only requires *express* commitment, but also *conduct* evidencing commitment to observe those standards.

38.92 In the ALRC's view, it would be desirable for the OPC, together with ACMA, to provide greater guidance to media organisations on appropriate levels of privacy protection and raise awareness that the media exemption is not a blanket exemption.

Proposal 38–2 In consultation with the Australian Communications and Media Authority and peak media representative bodies, the Office of the Privacy Commissioner should establish criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

Proposal 38–3 The Office of the Privacy Commissioner should issue guidelines containing the criteria for assessing the adequacy of media privacy standards established under Proposal 38–2.

Proposal 38–4 Section 7B(4)(b)(i) of the *Privacy Act* should be amended to provide that the standards must 'deal *adequately* with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters)'.

Proposal 38–5 The Office of the Privacy Commissioner should issue guidance to clarify that the term 'publicly committed' in s 7B(4) of the *Privacy Act* requires both:

(a) express commitment by a media organisation to observe privacy standards that have been published in writing by the media organisation or a person or body representing a class of media organisations; and

(b) conduct by the media organisation evidencing commitment to observe those standards.

147 See Proposal 60–8.

Adequacy of the self-regulatory and co-regulatory models

38.93 In 1997, the Senate Select Committee on Information Technologies was established to evaluate the appropriateness, effectiveness and privacy implications of the self-regulatory framework of the information and communications industries—including the print media, television, radio and telecommunications sectors.[148] The Committee found that there were numerous instances that question the success of self-regulation and co-regulation by the information and communications industries. It considered that the models for self-regulation should remain unchanged, but recommended that an independent statutory body—the Media Complaints Commission—be established as a single reference point to deal with all complaints against Australia's information and communications industries.[149]

38.94 Two other inquiries into the broadcasting media, the Productivity Commission inquiry into broadcasting services in Australia and the inquiry by the Australian Broadcasting Authority into commercial radio, also found flaws with the current self-regulatory models. In 1999, the Australian Broadcasting Authority conducted an investigation under the *Broadcasting Services Act* into allegations that financial arrangements were made between certain radio presenters and third parties. The Australian Broadcasting Authority concluded that agreements existed between certain radio presenters and third parties, and that they had influenced the content of the radio programs.[150] It found that there appeared to be a systemic failure to ensure the effective operation of self-regulation, particularly in relation to current affairs programs—including a lack of staff awareness of the codes of practice and of their implications.[151] The Australian Broadcasting Authority came to a preliminary view that there should be a standard designed to entrench the appropriate functions of the codes across the commercial radio industry.[152] It also proposed that the *Broadcasting Services Act* be amended, including by making compliance with the codes of practice a statutory licence condition, and additional administrative remedies to provide the Australian Broadcasting Authority with more flexible enforcement options.[153] The proposed legislative changes have since been introduced into the *Broadcasting Services Act*.[154]

38.95 In 1999, the Productivity Commission was asked to conduct an inquiry into broadcasting services and 'advise on practical courses of action to improve competition, efficiency and the interest of consumers in broadcasting services'.[155] In its report, the Productivity Commission recommended that the *Broadcasting Services Act* be amended to impose certain additional standard conditions on broadcasters' licences,

---

148 Parliament of Australia—Senate Select Committee on Information Technologies, *In the Public Interest: Monitoring Australia's Media* (2000).
149 Ibid, recs 1–4.
150 Australian Broadcasting Authority, *Commercial Radio Inquiry—Final Report of the Australian Broadcasting Authority* (2000), 25–42.
151 Ibid, 4, 65.
152 Ibid, 100.
153 Ibid, 101–102.
154 *Broadcasting Services Act 1992* (Cth) ss 44, 88, 92J, 100, 119 and pt 14D.
155 Australian Government Productivity Commission, *Broadcasting Inquiry Report* (2000), iv.

including a condition that the broadcasters must take reasonable steps to provide methods for handling complaints.[156]

> The Commission considers, for a co-regulatory system to work effectively, that the regulator should possess credible powers to penalise transgressors. The [Australian Broadcasting Authority] does not have such a credible threat for initial breaches of the codes. [157]

38.96 The Productivity Commission recommended that the co-regulatory scheme be amended to include additional sanctions, including the broadcasting of an on-air announcement of a breach finding and subsequent action during the relevant program or time slot. It also recommended that the Australian Broadcasting Authority be given the power to issue directions for action to broadcasters found in breach of a relevant licence condition.[158] Only the last recommendation has been implemented.[159]

38.97 The 2000 House of Representatives Committee inquiry acknowledged that the freedom of the press and the free flow of information to the public via the media are important elements of a democratic society. The inquiry, however, expressed concern at the enormous potential for breaches of privacy if media organisations or journalists behaved irresponsibly.[160] It recommended that journalists and media organisations be required to subscribe to a code developed by a media organisation, a representative body or the Privacy Commissioner before they can take advantage of the exemption.[161] The AGD opposed this recommendation.[162]

38.98 One commentator argues that the current self-regulatory model should remain.[163] In his view, the only practical alternative is a government-appointed body, but contends that this would be undesirable because the right to publish freely without fear of government intervention is fundamental to a democratic society.[164]

---

156 Ibid, 456.

157 Ibid, 479.

158 Ibid, rec 13.7.

159 *Broadcasting Services Act 1992* (Cth) s 141.

160 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [4.47]–[4.48].

161 Ibid, rec 9. The Committee also recommended that the Privacy Commissioner conduct an education campaign to inform the public about the special provisions applying to the media: Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), rec 10.

162 Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000) <www.ag.gov.au> at 1 August 2007.

163 D Pearce, 'Privacy and the Press: Issues of Balance and Perspective' (2003) 10 *Privacy Law & Policy Reporter* 132, 138. This was supported in one submission: Australian Press Council, *Submission PR 48,* 8 August 2006.

164 D Pearce, 'Privacy and the Press: Issues of Balance and Perspective' (2003) 10 *Privacy Law & Policy Reporter* 132, 138.

Overseas jurisdictions

38.99 A number of overseas jurisdictions also adopt the self-regulatory model for the print media and the co-regulatory model for the broadcast media. For example, in the United Kingdom, the print media are self-regulated and overseen by the Press Complaints Commission. The Press Complaints Commission is an industry body that deals with complaints from members of the public about the editorial content of newspapers and magazines.[165] In relation to the broadcasting media, the Office of Communications was established under the *Office of Communications Act 2002* (UK) as the regulator for the UK communications industries.[166] It applies a single *Broadcasting Code* across the broadcasting industry.[167] The Office of Communications is charged with handling and adjudicating privacy complaints under s 326 of the *Communications Act 2003* (UK).

38.100 The New Zealand print media is also self-regulatory. It is overseen by the New Zealand Press Council, a private body established in 1972 by newspaper publishers and journalists to provide an independent forum for the resolution of public complaints.[168] The broadcast media are subject to higher regulatory standards, pursuant to a co-regulatory model under the *Broadcasting Act 1989* (NZ). The Act establishes the Broadcasting Standards Authority as a supervisory body whose functions include: receiving and determining complaints; encouraging the development and observance by broadcasters of codes of practice in relation to individual privacy; approving codes; and developing and issuing codes itself where it considers that it is appropriate to do so.[169]

Submissions and consultations

38.101 In IP 31, the ALRC asked how journalistic acts and practices should be regulated if the media exemption is retained.[170] A number of media organisations and their representative bodies submitted that the current regulatory model should remain.[171] It was submitted that the advantages of self-regulation are that: it is inexpensive and efficient;[172] and the newspaper and magazine publishing industry is committed to it and agrees to abide by the APC's rulings to publish adjudications where appropriate.[173]

---

165 United Kingdom Press Complaints Commission, *What is the PCC?* <www.pcc.org.uk/about/whatispcc.html> at 6 August 2007.

166 United Kingdom Office of Communications, *Statutory Duties and Regulatory Principles* <www.ofcom.org.uk/about/sdrp> at 16 August 2007.

167 United Kingdom Office of Communications, *Ofcom Broadcasting Code* (2005).

168 New Zealand Press Council, *Main* <www.presscouncil.org.nz> at 17 August 2007.

169 *Broadcasting Act 1989* (NZ) ss 20, 21(a), (e)(viii), (f), (g).

170 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–12.

171 Free TV Australia, *Submission PR 149,* 29 January 2007; SBS, *Submission PR 112,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

172 Free TV Australia, *Submission PR 149,* 29 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

173 Australian Press Council, *Submission PR 83,* 12 January 2007.

38.102 Some stakeholders submitted that a body appointed by the government to oversee the media is undesirable,[174] as it would interfere with the right to publish freely without fear of government intervention, which is fundamental to a democratic society.[175] The APC further submitted that the government appointing a body to oversee the print media

> would contradict the basic tenet of press freedom in a liberal democracy: its independence from government so that it can adequately report and comment on government matters, a principle that the High Court identified as a significant feature of our democracy.[176]

38.103 It was also suggested in some submissions that the current regulatory framework already provides adequate protection for individual privacy,[177] as shown by the low number of privacy related complaints against the media.[178]

38.104 In contrast, the Legal Aid Commission of New South Wales submitted that 'alternative remedies under media self regulation are widely seen as lacking real independence or the ability to conduct investigations leading to definite findings'.[179] The New South Wales Council for Civil Liberties submitted that:

> There should also be a mechanism whereby individual complaints can be lodged and dealt with by an independent body and the conduct complained of open to some scrutiny and redress where appropriate.[180]

ALRC's view

38.105 In the ALRC's view, freedom of expression is a fundamental tenet of a liberal democracy. Appointing an independent government body to oversee the media is a measure of last resort. Such an approach should be taken only where there is substantial evidence that self-regulation and co-regulation in the media industry have failed. Based on the relatively low rate of privacy-related complaints, investigations and findings of breach, as well as the small number of submissions calling for a change in regulatory model, the ALRC does not consider that the appointment of a government body, such as a Media Complaints Commission, is warranted.

---

174 SBS, *Submission PR 112,* 15 January 2007; Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

175 Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007; Australian Press Council, *Submission PR 83,* 12 January 2007.

176 Australian Press Council, *Submission PR 83,* 12 January 2007. See also Australian Broadcasting Corporation, *Submission PR 94,* 15 January 2007.

177 Free TV Australia, *Submission PR 149,* 29 January 2007; SBS, *Submission PR 112,* 15 January 2007.

178 Free TV Australia, *Submission PR 149,* 29 January 2007.

179 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

180 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

Enforcement mechanisms

38.106 Concerns have been raised about the lack of adequate enforcement mechanisms for media privacy standards. For example, one commentator criticised the fact that the only mechanism for ensuring compliance with the APC's *Privacy Standards* is the complaint process of the APC**,** which only has jurisdiction over members who have voluntarily accepted it.[181] In addition, it has been argued that the 'penalty' imposed by the APC is not a deterrent.[182]

Submissions and consultations

38.107 A number of media organisations and media representative bodies submitted that the mechanisms to enforce media privacy standards are working well.[183]

38.108 In relation to the print media, the APC acknowledged that 'as the Council has no powers to fine or prosecute publications or force them to publish corrections or apologies, it has, on occasion, been branded a "toothless tiger"'. It suggested, however, that:

> This absence of punitive powers is, in fact, the Council's most beneficial strength. As a self-regulating body, newspapers and magazines have agreed to cooperate with the Council in resolving complaints quickly and at no expense to the complainant. They agree to abide by the Council's rulings and to publish adjudications where appropriate. [184]

38.109 The APC also submitted that its experience with administrating the *Privacy Standards* has been positive, and that fewer than 5% of complaints to the APC were about invasion of privacy. It stated that none of the individuals that comprise the APC Secretariat has a background in journalism and the staff members primarily responsible for the processing of complaints are trained mediators. Further, 'when complaints are referred to the Council for adjudication, the Council includes representatives of the publishers, independent journalists and members of the public'. According to the APC, there have been 22–25 complaints to the APC on privacy matters annually since 2001, and that:

> The overwhelming majority of complaints are settled by conciliation, early in the process, and those settled by adjudication do not demonstrate any egregious abuse of citizens' privacy rights.[185]

38.110 In relation to the broadcasting industry, it was suggested in some submissions that the enforcement mechanism is adequate. ACMA submitted that:

---

181 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.
182 Ibid.
183 Australian Press Council, *Submission PR 83,* 12 January 2007; Australian Press Council, *Submission PR 48,* 8 August 2006.
184 Australian Press Council, *Submission PR 83,* 12 January 2007.
185 Australian Press Council, *Submission PR 48,* 8 August 2006.

> This new power [under the *Communications Legislation Amendment (Enforcement Powers) Act 2006* (Cth)] will increase the range of appropriate sanctions and regulatory responses available to ACMA in dealing with breaches of broadcasting codes, including privacy-related breaches.[186]

38.111 Free TV Australia submitted that the provisions of the various industry codes of practice 'are overseen and administered by a federal regulator that has specific knowledge and understanding of the media industry'.[187]

38.112 In contrast, it was submitted that at least some of the current media privacy standards lack strong enforcement mechanisms.[188] One submission stated that 'the APC lacks enforcement powers other than publication of findings of non-compliance'.[189] The New South Wales Council for Civil Liberties Inc submitted that 'there should be some effective sanctions to operate as a disincentive to abuse of the media's freedom to report', which may be of a monetary or non-monetary kind.[190]

ALRC's view

38.113 Some of the media privacy standards do not have strong enforcement mechanisms. While ACMA now has legislative power to impose a range of sanctions, the APC can only publish its findings of non-compliance, and the Media Entertainment and Arts Alliance has a limited range of remedies and no power to act against or sanction a non-member. The ALRC considers that the proposed criteria for assessing the adequacy of media privacy standards discussed above should help to address the issue of adequate enforcement powers and sanctions. The adequacy of enforcement powers and sanctions would be a consideration when determining whether media privacy standards are adequate. Where the media privacy standards are inadequate, the media exemption would not apply.

---

186 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.
187 Free TV Australia, *Submission PR 149,* 29 January 2007.
188 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
189 Ibid.
190 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

39. Other Private Sector Exemptions

Contents

Introduction 1113
Personal or non-business use 1113
Related bodies corporate 1115
Submissions and consultations 1118
ALRC's view 1120
Change in partnership 1121
Submissions and consultations 1121
ALRC's view 1122

Introduction

39.1 The preceding chapters examined a number of the major private sector exemptions from the *Privacy Act 1988* (Cth) (*Privacy Act*). This chapter considers the remaining private sector exemptions relating to personal, family or household affairs; related bodies corporate and change in partnership; and the circumstances under which overseas acts and practices of an organisation are excluded from the coverage of the privacy principles.

Personal or non-business use

39.2 Individuals are included in the definition of an 'organisation' in the *Privacy Act*.[1] Section 7B(1) of the Act provides that acts and practices of individuals are exempt if they are done *other than* in the course of business. Section 16E further provides that the National Privacy Principles (NPPs) do not apply where information is dealt with solely in the context of an individual's personal, family or household affairs.

39.3 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) stated that the *Privacy Act* was not intended to affect the way individuals handle personal information in the course of their personal, family or household affairs.[2] It also stated that the purpose of s 16E was to confirm that the NPPs do not apply where information is dealt with in the context of an individual's personal,

1 *Privacy Act 1988* (Cth) s 6C(1)(a).
2 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [106].

family or household affairs, consistently with s 7B(1). It appears from the Revised Explanatory Memorandum that 'personal, family or household affairs' has the same meaning as 'other than in the course of business'.[3]

39.4 There is no express reference to 'personal, family or household affairs' or similar in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* issued by the Organisation for Economic Co-operation and Development (OECD Guidelines).[4] The Guidelines do, however, appear to recognise that the collection of personal information in the context of an individual's personal affairs should be excluded from its application. OECD Guideline 2 provides that the Guidelines are only intended to

> apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.[5]

39.5 The Memorandum to the OECD Guidelines goes on to state that 'the risks as expressed in [OECD Guideline 2] are intended to exclude data collections of an obviously innocent nature (for example, personal notebooks)'.[6]

39.6 Both the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework provide that they do not apply to the handling of personal information in connection with an individual's personal or household affairs. Article 3(2) of the EU Directive provides that 'this Directive shall not apply to the processing of personal data … by a natural person in the course of a purely personal or household activity'.[7] Similarly, the APEC Privacy Framework defines 'personal information controller' as excluding 'an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs'.[8]

39.7 The European Court of Justice has interpreted the exemption under art 3(2) of the EU Directive as 'relating only to activities which are carried out in the course of

---

3 Ibid, notes on clauses [164].

4 Privacy legislation in some overseas jurisdictions uses expressions that are similar to 'personal, family or household affairs', eg, 'personal or domestic purposes' (*Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4(2)(c)); 'personal or domestic activities' (*Federal Data Protection Act 1990* (Germany) ss 1(2), 27).

5 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 2.

6 Ibid, Memorandum, [43].

7 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 3(2). See also European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recital 12.

8 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].

private or family life of individuals', and not 'publication on the internet so that those data are made accessible to an indefinite number of people'.[9]

39.8 An exemption for personal, family or household affairs is commonly provided for in overseas jurisdictions, for example, the United Kingdom, Canada, New Zealand and Hong Kong.[10]

39.9 Privacy concerns about the exemption arise primarily in the context of developments in technology. For example, in its submissions to previous inquiries, the Australian Privacy Foundation suggested that this exemption needs to be reconsidered due to increasing incidents of abuse, including 'inappropriate use of mobile phone cameras and misguided and extremely prejudicial "vigilante" websites'.[11] During this Inquiry, much of the concern about individuals acting in their personal capacity relates to information posted by individuals on websites, such as the posting of photographs and offensive comments on websites and 'blogs'.[12] Options for reform in this area are considered in Chapter 8.

Related bodies corporate

39.10 An act or practice is not an interference with privacy if it consists of the collection or disclosure of personal information by a body corporate from or to a related body corporate.[13] The exemption does not extend to 'sensitive information',[14] which is defined to include health and personal information such as an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual preferences and criminal record.[15]

39.11 The stated reason for this exemption is to 'recognise [the] commercial reality that, for many bodies corporate to continue to operate effectively, they need to be able to communicate with related bodies corporate'.[16]

---

9 *Criminal Proceedings against Bodil Lindqvist* [2003] I ECR 12971, [47].

10 *Data Protection Act 1998* (UK) s 36; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 4; *Privacy Act 1993* (NZ) s 56; *Personal Data (Privacy) Ordinance* (Hong Kong) s 52.

11 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.

12 See, eg, Confidential, *Submission PR 49,* 14 August 2006. A 'blog' is a shortened form of web log. It means a record of items of interest found on the internet, edited and published as a website with comments and links; or a personal diary published on the internet: *Macquarie Dictionary* (online ed, 2005).

13 *Privacy Act 1988* (Cth) s 13B(1).

14 Ibid s 13B(1).

15 Ibid s 6(1).

16 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [138].

39.12 Section 6(8) of the *Privacy Act* provides that 'the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the *Corporations Act 2001* [(Cth)]'. A 'related body corporate' is defined in s 50 of the *Corporations Act* to mean that where a body corporate is a holding company of another body corporate, a subsidiary of another body corporate, or a subsidiary of a holding company of another body corporate, the first mentioned body and the other body are related to each other. Before an organisation can rely on this exemption to disclose non-sensitive personal information to other related companies, it is required to take reasonable steps to ensure that the individual knows that the organisation has collected the information, the use that will be made of the information and the types of organisations to which the information is usually disclosed.[17]

39.13 In addition, although related companies may share personal information, the handling of that information is still subject to the NPPs in other respects.[18] For example, each company within the group of related companies must use the information consistently with the primary purpose for which it was originally collected, and may use the personal information for a secondary purpose only where that purpose is allowed by NPP 2.1.[19]

39.14 The way the exemption operates may be illustrated by the following example. A large furniture store collects an individual's credit card details to receive payment for a sofa, and the individual's name and address in order to deliver the sofa. The related body corporate exemption allows the furniture store to pass on the individual's name, address and credit card details to a related delivery company. The delivery company is allowed to collect the information from the furniture company without having to inform the individual that it has collected that information. The delivery company can use this personal information only for the purpose for which the furniture store collected it (ie, delivery of the sofa). It cannot use the information for an unrelated purpose.[20]

39.15 The exemption does not apply to the collection of personal information from an entity that is exempt from the requirement to comply with the *Privacy Act*.[21] For example, a company that is related to a media organisation (which is exempt from the operation of the *Privacy Act* where it is acting in the course of journalism under certain conditions)[22] cannot rely on s 13B to collect personal information from the media organisation without complying with the requirement, in NPP 1.5, to take reasonable

---

17 Ibid, notes on clauses [139].

18 *Privacy Act 1988* (Cth), note to s 13B(1); Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [141].

19 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [141].

20 The information can be used for a secondary purpose that is permitted by NPP 2.1, such as direct marketing.

21 *Privacy Act 1988* (Cth) s 13B(1A)(a), (b).

22 Ibid s 7B.

steps to ensure that individuals are aware of certain matters before collecting that information.[23]

39.16 Section 13B(2) of the *Privacy Act* provides that the exemption does not apply if the company is a contractor under a Commonwealth contract and: the collection or disclosure of personal information from or to the related company is contrary to a contractual provision; or the collection of personal information is for the purpose of meeting an obligation under the contract and the disclosure is for direct marketing purposes.[24] The purpose of s 13B(2) is to ensure that the exemption 'does not override the general rule for organisations that are contracted service providers'.[25]

39.17 Furthermore, the exemption does not apply if the acts and practices of the company: breach the tax file number (TFN) guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; contravene Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or the data-matching guidelines made under that Act; constitute a breach of the guidelines under s 135AA of the *National Health Act 1953* (Cth); or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[26]

39.18 An inquiry into the Privacy Amendment (Private Sector) Bill by the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry accepted that many businesses are structured in a way that uses more than one legal entity. The Committee acknowledged that the exact structure of many businesses may not be apparent to consumers. In the Committee's view, this justifies requiring companies to provide greater information about the likely use of the data collected, rather than preventing them from sharing information with other members of their corporate groups.[27] The inquiry therefore recommended that the Privacy Commissioner establish guidelines for use by companies to determine the extent of information they should provide to consumers about the nature of their corporate groups and the information to be shared within the members of that group.[28]

39.19 This exemption has been criticised as a potential loophole through which corporate groups could evade the coverage of the *Privacy Act*.[29] In its submissions to previous inquiries, Electronic Frontiers Australia submitted that the exemption enables large businesses intentionally to structure their affairs to take advantage of the

---

23 See Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [142].

24 *Privacy Act 1988* (Cth) s 13B(2).

25 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [143]. Privacy issues concerning contracted service providers are discussed in Ch 11.

26 *Privacy Act 1988* (Cth) s 13E.

27 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [9.21].

28 Ibid, rec 21.

29 Ibid, [9.9].

exemption. In its view, individuals should not have to ask or attempt to investigate corporate structures to find out how far and wide their personal information could be spread. Electronic Frontiers Australia submitted that the exemption should be removed and related bodies corporate treated as third parties.[30]

39.20 Another issue arises in relation to the interaction between the exemption for related companies and NPP 9. NPP 9 outlines the circumstances in which an organisation can transfer personal information outside Australia. This issue is discussed in Chapter 28.

Submissions and consultations

39.21 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether there are any issues concerning related bodies corporate in Part III Division 1 of the *Privacy Act*, and if so, how they should be dealt with.[31]

39.22 Some stakeholders submitted that the exemption should be removed, on the basis that individuals often are not aware that an organisation is related to another organisation. This results in use of information that is contrary to the reasonable expectations of individuals.[32] It was suggested that businesses should be able to meet one of the tests in the exceptions to the use and disclosure principle in NPP 2 without the need for a special exemption.[33]

39.23 Stakeholders also expressed concern that the exemption may allow personal information about an individual to be used for direct marketing by related bodies corporate without the individual's knowledge or consent. While the Queensland Council for Civil Liberties did not object to the exemption, it suggested that:

> the principle should be amended to prevent direct marketing that is contrary to the individuals' reasonable expectation at the time of the original collection of the personal information.[34]

39.24 The Queensland Government Commissioner for Children and Young People and Child Guardian submitted that when children and young people subscribe to mobile phone networks or register for online subscriptions, the sharing of non-sensitive information between related companies may make them susceptible to direct

---

30 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004; Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005.

31 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–8.

32 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007, referring to Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005.

33 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

34 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

marketing. It suggested that 'permission should be sought from children and young people before their personal information is shared between associated organisations'.[35]

39.25 In its submission, the Office of the Privacy Commissioner (OPC) noted that:

> The Office has received complaints from time to time from individuals that their information has been used for direct marketing by a related body corporate without their knowledge or consent. The Office submits that improved notice of disclosure by the relevant body corporate under NPP 1.3 should ameliorate this concern.[36]

39.26 In contrast, some stakeholders considered that the sharing of customers' personal information between related bodies corporate did not raise any issues.[37] In addition, Telstra submitted that the exemption is 'necessary for efficient and effective business practices'. It noted that large organisations provide services to, and contract with, customers through different legal entities for various business purposes and to comply with legislative requirements. Telstra stated:

> Restricting the ability of such organisations to exchange personal information will hinder business operations and cause detriment to consumers by making it more difficult for businesses to contract with their customers in a consistent manner.[38]

39.27 The Australian Bankers' Association Inc (ABA) submitted that while a bank sharing customers' personal information with a related entity is constrained by the bank's duty of confidentiality, the exemption is required when a related entity that is not a bank provides its customers' information to the bank. It noted that a company that collects personal information from a related company is bound by the NPPs as if it were the original collector of the information. In addition, the ABA stated that it was

> unaware of any customer concerns over the sharing of customers' personal information with related entities of banks and this is borne out by the relatively low level of privacy related disputes that the Banking and Financial Services Ombudsman scheme (BFSO) receives in a year …[39]

39.28 The Law Council of Australia suggested that 'the need for commercially efficient inter-company transfers applies equally to transfers of information overseas'. It submitted that the exemption should be extended to transfers of information to a related body corporate overseas—provided that the related body corporate has an organisational link with Australia and, therefore, is subject to the jurisdiction of the *Privacy Act*.[40]

---

35 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

36 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

37 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Telstra, *Submission PR 185,* 9 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

38 Telstra, *Submission PR 185,* 9 February 2007.

39 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

40 Law Council of Australia, *Submission PR 177,* 8 February 2007.

ALRC's view

39.29 The ALRC agrees with the conclusion of the 2000 House of Representative Committee inquiry that, in the interest of business efficacy, companies that have a shared ownership or controlling interest should be able to share non-sensitive personal information.

39.30 The exemption is a limited one. First, it is confined to non-sensitive personal information. Secondly, the exemption does not apply to the collection of personal information from an entity that is exempt from compliance with the *Privacy Act*. In addition, before an organisation can disclose such information to other related companies, it must take reasonable steps to ensure that individuals know the types of organisations to which the information is usually disclosed. Finally, although related companies may share non-sensitive personal information, they must otherwise comply with all the other privacy principles in the handling of that information.

39.31 A concern has been raised about the use of personal information by a related company for direct marketing purposes. As discussed above, the OPC has suggested that an improved notice of disclosure by the relevant body corporate could ameliorate this concern. Currently, NPP 1.3(d) requires an organisation to take reasonable steps to ensure that an individual is aware of the organisations or types of organisations to which the information is usually disclosed. The ALRC does not consider that requiring a more detailed notice of disclosure—for example, one that lists all related companies by name—would adequately address concerns about direct marketing. In practice, individuals may not be interested in reading a long list of related companies or keeping a copy of that list for later reference.

39.32 A better alternative is to provide individuals with the means to opt out of direct marketing. In Chapter 23, the ALRC proposes that an organisation involved in direct marketing be required to: take reasonable steps, upon request, to advise the individual from where it acquired the individual's personal information; and present individuals with a simple means to opt out of receiving direct marketing communications. These proposals should help ensure that individuals are able to opt out of direct marketing from a related company to whom their personal information is disclosed.

39.33 In relation to concerns about direct marketing to children and young people, in Chapter 23 the ALRC proposes that the OPC issue guidance to organisations involved in direct marketing that clarifies their obligations under the *Privacy Act* in dealing with particularly vulnerable people, such as individuals aged 14 and under.[41] This should assist organisations in understanding when it is appropriate to communicate with such individuals by way of direct marketing.

---

41 See Proposal 23–6(b).

Change in partnership

39.34 In certain circumstances, an act or practice is not an interference with the privacy of an individual if it consists of passing personal information from an old to a new partnership.[42] The new partnership must: be formed at the same time or immediately after the old one; have at least one partner transferred from the old partnership; and carry on the same or a similar business as the old partnership.[43] The exemption applies to the disclosure and collection of personal information between the old and new partnerships, but does not apply to the use and holding of the information.[44]

39.35 The exemption does not apply if the acts and practices: breach the TFN guidelines, or involve an unauthorised requirement or request for disclosure of an individual's TFN; breach Part 2 of the *Data-matching Program (Assistance and Tax) Act* or the data-matching guidelines made under that Act; constitute a breach of the guidelines under s 135AA of the *National Health Act*; or constitute a credit reporting infringement by a credit reporting agency or a credit provider.[45]

39.36 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill gave the following example to illustrate the reason for the exemption:

> For example, a law firm (a partnership) collects personal information from, and holds personal information about, its clients. If a partner leaves the partnership, and a new partner joins the firm, the first partnership has dissolved and a second partnership forms. The purpose of clause 13C is to prevent disclosure to the second partnership and collection by the second partnership from being an interference with privacy. The sub-clause is not intended to allow a partnership to reform and use the information collected for a totally different business purpose.[46]

Submissions and consultations

39.37 In IP 31, the ALRC asked whether there are any issues concerning changes in partnership in Part III Division 1 of the *Privacy Act*, and if so, how they should be dealt with.[47] The OPC stated that where there is a change in partnership that falls within the exemption,

> as a matter of best practice … [the] new partnership should write to their customers and advise them of the change. In this way the individual concerned has a measure of choice over whether they wish to continue to transact with the new partnership and in

---

42 *Privacy Act 1988* (Cth) s 13C.
43 Ibid s 13C(1).
44 Ibid, note to s 13C(1).
45 Ibid s 13E.
46 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [144].
47 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–8.

this way have some control over their personal information that the partnership has collected.[48]

ALRC's view

39.38 Partnership law provides that, subject to the terms of the specific partnership agreement, an old partnership is dissolved and a new partnership is created whenever a partner joins or leaves a partnership.[49] In the ALRC's view, the exemption is a sensible approach to avoid an unnecessary burden on partnerships to obtain consent from individuals for the transfer of their personal information from the old partnership to the new one each time a partner joins or leave a partnership. It should be noted that, except for the transfer of personal information from the old partnership to the new one, the partnership must continue to comply with the privacy principles in all other respects.

39.39 The ALRC agrees with the OPC that it is desirable for the new partnership to write to their customers to advise them of the change. This should be a matter of good practice rather than a formal statutory requirement.

---

48 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

49 *Partnership Act 1892* (NSW) ss 24(1)(7), 26, 32, 33; *Partnership Act 1891* (Qld) ss 27(1)(g), 29, 35, 36; *Partnership Act 1958* (Vic) ss 28(7), 30, 36, 37; *Partnership Act 1895* (WA) ss 35(6), 43, 44; *Partnership Act 1891* (SA) ss 24(1)(g), 26, 32, 33; *Partnership Act 1891* (Tas) ss 29(g), 31, 37, 38; *Partnership Act* (NT) ss 28(1)(g), 30, 36, 37; *Partnership Act 1963* (ACT) ss 29(7), 31, 37, 38.

40. New Exemptions

Contents

Introduction 1123
New exemptions and partial exemptions 1123
Private investigators 1124
Valuers 1129
Archivists and archival organisations 1132
Alternative dispute resolution bodies 1132
Declared emergencies 1137

Introduction

40.1 This chapter discusses possible new exemptions from the requirements of the *Privacy Act 1988* (Cth). New exemptions or partial exemptions (or exceptions)[1] have been suggested in relation to the information-handling practices of private investigators, valuers, professional archivists and archival organisations, and alternative dispute resolution (ADR) bodies.

40.2 The chapter also discusses the partial exemption contained in Part VIA of the Act relating to declared emergencies, which came into operation in December 2006. Part VIA displaces some of the requirements in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) by providing a separate regime for the collection, use and disclosure of personal information where there is a connection to an emergency that has been the subject of a declaration by the Prime Minister or a minister.

New exemptions and partial exemptions

40.3 In the ALRC's Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether there are any other entities or types of activities that should be exempt from

1 For the purposes of this Discussion Paper, an exemption applies where a specified entity or a class of entity is not required to comply with the privacy principles. A partial exemption applies where a specified entity or a class of entity is required to comply with either: (1) only some, but not all, of the privacy principles; or (2) some or all of the privacy principles, but only in relation to certain of its activities. An exception applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. This distinction is discussed in more detail in Ch 30.

the operation of the *Privacy Act*; and if so, what those entities or types of activities are, and what the scope of the exemption should be.[2]

40.4 Some stakeholders submitted that there is no case for introducing new exemptions from the operation of the *Privacy Act*.[3] For example, the Office of the Privacy Commissioner (OPC) stated:

> The Office is not aware of a compelling case for any other entities or types of activities, including that of valuers, should be exempt from the operation of the Privacy Act. The Office takes the view that to achieve uniformity and consistency of application of privacy legislation, exemptions under the Privacy Act should be minimised. Where they exist, there should be a clear public interest enunciated for any exemption to be maintained or created.[4]

40.5 The Australian Privacy Foundation stated:

> We do not see the need for any total exemptions, and are not aware of any other entities or types of activities which need selective exceptions. Carefully designed selective exceptions should be able to accommodate any new or currently unrecognised compliance difficulties.[5]

40.6 Other stakeholders suggested new exemptions or partial exemptions in relation to the information-handling practices of private investigators, valuers, professional archivists and archival originations, and ADR bodies. These possible exemptions are discussed below.

Private investigators

40.7 Private investigators provide investigative and legal support services to government agencies, corporate entities and the public in areas that are said to include: fraud prevention, detection, assessment and resolution; corporate fraud and risk management services; insurance fraud and claims investigation, claims monitoring and assessment; aviation accident and loss investigation; marine loss investigations; occupational health and safety incident investigation; witness location and skip tracing; criminal investigations; child protection investigations; investigative journalism; family law investigations; intellectual property protection services; background checking; consumer investigations; and missing person investigations.[6]

40.8 Most states and territories have statutory schemes for licensing private investigators. Licences are granted in New South Wales, Victoria, Queensland,

---

2 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 5–14.

3 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

4 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

5 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. Also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

6 Australian Institute of Private Detectives Ltd, *Code of Practice for Private Investigators in Australia* (2005), 5.

Western Australia, South Australia, Tasmania and the Northern Territory.[7] Typically, such legislation provides for:

- Threshold requirements for granting a licence—such as minimum age, completion of an approved training course, and absence of convictions in relation to disqualifying offences (as defined in the legislation) which automatically disentitle a person to hold a licence.

- Discretionary considerations for granting a licence—such as appropriateness or fitness to hold a licence, character, previous conduct (including criminal association), previous convictions or findings of guilt, and public interest considerations.

- Licensing offences—including offences in relation to practising without a licence; holding oneself out as having a licence; delegating work to an unlicensed person; improperly obtaining a licence; disposing of licences through sale, loan or gift; and exceeding licence conditions.

40.9 There are many differences, however, between state and territory schemes for licensing private investigators. Major differences include those in relation to the nature of offences that automatically disentitle an applicant from holding a licence; qualifications and training requirements; and penalties for licensing offences. In this context, the Australian Institute of Private Detectives (AIPD) has prepared a draft bill to indicate how uniform national regulation of private investigation might be enacted.[8] The draft bill is based on the *Commercial Agents and Private Inquiry Agents Act 2004* (NSW).

40.10 Private investigators may also be subject to various industry self-regulatory schemes. For example, the AIPD requires its members to be bound by an AIPD Code of Practice, Code of Ethics, standards and guidelines.[9] The only sanction for a breach of these requirements, however, is the cancellation a person's membership. The AIPD does not have any power to remove a person's licence to practise as a private investigator.

---

7 *Commercial Agents and Private Inquiry Agents Act 2004* (NSW); *Private Agents Act 1996* (Vic); *Security Providers Act 1993* (Qld); *Security and Investigation Agents Act 1995* (SA); *Security and Related Activities (Control) Act 1996* (WA); *Security and Investigations Agents Act 2002* (Tas); *Commercial and Private Agents Licensing Act 1979* (NT).

8 Australian Institute of Private Detectives, *Private Investigators Bill 2005* <www.aipd.com.au> at 14 August 2007.

9 Australian Institute of Private Detectives Ltd, *Code of Practice for Private Investigators in Australia* (2005), 22.

Private investigation and the Privacy Act

40.11 The *Privacy Act* makes no specific provision for the activities of private investigators. Private investigators are generally required to comply with the NPPs, even where they are small businesses—the small business exemption[10] does not generally apply to organisations that trade in personal information.[11]

40.12 Various aspects of the operation of the *Privacy Act* that might be seen as unduly hampering the activities of private investigations were highlighted in the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review).[12]

40.13 For example, one concern for private investigators is the obligation, under NPP 1.5, to take reasonable steps to make individuals aware that a private investigator is collecting information about them. In this context, the OPC noted that the 'reasonable steps' required by the privacy principle could include taking no steps, where, for example, a suspicion of fraud or unlawful activity is being investigated.[13]

40.14 On the other hand, where investigators are investigating activity that is 'improper rather than unlawful'—for example, 'misuse of employer resources, abuse of power or position, or marital infidelity' complying with the collection principle 'may impinge on the activities of private investigators'.[14] The OPC observed that:

> it is considerably less clear in these circumstances that the public interest in investigating possibly improper activity outweighs the individual and the public interest in individuals being aware that they are under investigation.[15]

40.15 In the OPC Review, the AIPD and others submitted that NPP 2 severely hampers the activities of private investigators because it prohibits organisations from disclosing information to private investigators, including information necessary for debt collection,[16] service of legal process, and fraud investigation.[17] A particular concern was that, while the *Privacy Act* facilitates access to personal information by law enforcement bodies, no such access is available to private investigators, including those who may be engaged by defendants or others who are subject to law enforcement action.

---

10 See Ch 35.

11 That is, collect personal information about another individual from, or disclose such information to, anyone else for benefit, service or advantage (unless it always has the consent of the individuals concerned, or only does so when authorised or required by law): *Privacy Act 1988* (Cth) s 6D(7), (8).

12 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).

13 Ibid, 225.

14 Ibid, 226.

15 Ibid, 226.

16 The disclosure of credit reporting information for debt collection purposes is discussed in Ch 53.

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 226.

40.16 On the other hand, the OPC has observed that there are important distinctions between public law enforcement agencies and private investigators. Notably, while law enforcement agencies carry out investigations on behalf of the state, private investigators carry out investigations on behalf of third parties, who are often private individuals.

> Giving private investigators access to personal information in this way could mean that they are carrying out investigations without the important scrutiny and accountability mechanisms that law enforcement agencies are subject to.[18]

Industry view

40.17 The AIPD submitted to the OPC Review that the definition of 'enforcement body' in s 6 of the *Privacy Act* should be amended to include 'private investigators in relation to matters before courts or tribunals'.[19] The effect of this would be to allow disclosure of personal information to a private investigator under NPP 2.1(h)(v), where disclosure is reasonably necessary for the preparation for proceedings before a court or tribunal.

40.18 The AIPD also referred to the model provided by an exemption from non-disclosure provisions contained in the *Data Protection Act 1998* (UK).[20] Section 35 of the *Data Protection Act* provides that:

> (2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary—
>
> (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
>
> (b) for the purpose of obtaining legal advice,
>
> or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

40.19 The Institute of Mercantile Agents, in a submission to the ALRC's Inquiry, did not favour an exemption for private investigation but stated that:

> There should be prescribed access allowing the genuine use of locator data held by licensed operatives (collection, credit and investigations) under State and Federal legislation …[21]

ALRC's view

40.20 Private investigators have a legitimate role in providing investigative and legal support services in a range of contexts. There is, for example, a social interest in

---

18 Ibid, 229.
19 Ibid, 229.
20 Australian Institute of Private Detectives, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.
21 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

individuals being able to take effective action to recover debts owed to them, find a person who is at fault in a car accident, and prepare a defence case for court proceedings.[22] In some instances, private investigators may perform tasks that could be done by the police or other law enforcement bodies, if resources and priorities permitted.

40.21 The activities of private investigators are often dependent on an ability to obtain access to personal information. The ALRC recognises that the *Privacy Act*, and state and territory privacy legislation, present obstacles to private investigators in obtaining personal information. A sufficient case has not been made, however, for proposing that an exemption (or other special provisions) directed towards private investigation be incorporated in the *Privacy Act*.

40.22 The ALRC is inclined to agree with the conclusion of the OPC Review that it would be difficult to recommend that private investigators be accorded similar access rights to personal information as law enforcement agencies.

> Private detectives can be distinguished from other enforcement bodies on the basis that they are not accountable to the government or the community, or any accountability body such as an ombudsman who can investigate complaints and award compensation, in the same way that law enforcement agencies are.[23]

40.23 One view is that, if the investigations industry were to be regulated more stringently, this might justify some special recognition of the position of private investigators under privacy law. Research reported in 2001 concluded that the industry would support 'tougher licensing, especially in pre-service training requirements' in return for an enhanced capacity to access information relevant to investigations.[24]

> Private investigators want a more active regulatory regime with more proactive auditing of firms, and more comprehensive consultation and communication with licence holders.[25]

40.24 Broader issues concerning the regulation of the private investigation industry including, for example, new national licensing and accountability mechanisms, are beyond the Terms of Reference of this Inquiry. Issues concerning regulation of the private investigation industry may, however, be an appropriate subject for consideration by the Standing Committee of Attorneys-General (SCAG). The OPC Review recommended that SCAG consider issues raised by the AIPD, which included

---

22 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 230.

23 Ibid, 230.

24 T Prenzler, *Private Investigators in Australia: Work, Law, Ethics and Regulation* (2001) Criminology Research Council, 6.

25 Ibid, 6.

the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry.[26]

> **Question 40–1** Should the Australian Government request that the Standing Committee of Attorneys-General consider the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry?

Valuers

40.25 Valuers assess the value of properties, including residential, commercial, industrial and retail properties. They may be engaged by private parties, corporations, financial institutions, or government departments and authorities. Private sector valuers are required to comply with the NPPs. Some state and territory legislation also regulates the handling of personal information by valuers.[27]

40.26 In its submissions to this Inquiry, the Real Estate Institute of Australia (REIA) proposed an exemption for valuers under the *Privacy Act*. In its view, there is an overwhelming public need for accurate, up-to-date and reliable property information for the purposes of making appraisals and preparing valuation reports. It submitted that the ability of valuers to collect up-to-date and reliable personal and property information has been diminished by the *Privacy Act*.[28] The REIA stated that this

> lessens the quality and accuracy of their professional advice to financiers, businesses and consumers, which in turn places them at risk. These risks can be measured in terms of increased financial burdens, uncertainty in property values and investment potential, and flawed land tax and stamp duty assessments. Valuers will also be the subject of increasing litigation.[29]

40.27 The REIA noted that, under NPP 2.1, real estate agents may only disclose personal information relating to property transactions where consent has been granted

---

26 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 231.

27 *Valuers Regulation 2005* (NSW) sch 2, r 9. For contract valuers engaged by state Valuers-General, see *Valuation of Land Act 1916* (NSW) s 11; *Valuation of Land Act 1978* (WA) ss 13, 14, 16; *Valuation of Land Act 2001* (Tas) ss 8, 53. For specialist retail valuers who are supplied information by landlords or tenants for the purposes determining the amount of rent under retail shop leases, see *Retail Leases Act 1994* (NSW) ss 19A(2), 31A(2); *Retail Leases Act 2003* (Vic) s 38; *Retail Shop Leases Act 1994* (Qld) s 35; *Business Tenancies (Fair Dealings) Act 2003* (NT) s 31.

28 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

29 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

or where the individual to whom the information relates would reasonably expect that his or her information would be disclosed for this purpose.[30]

> Confusion about whether or not a particular agency is exempt under the Privacy Act or whether parties to a property transaction would reasonably expect an agent to disclose information to outside parties is leading to a situation wherein agents are refusing to provide such information to property valuers.[31]

40.28 In relation to the need to disclose the name of the vendor or purchaser, in addition to other transaction details, the REIA stated:

> The name of the person is not always required when determining market values and comparable prices, however, for the purposes of valuation sometimes it is necessary. For example, the valuer needs to determine whether a property sale is at arms length (not an interrelated party or a forced sale) and hence at true market value. In a valuation report a person's name is removed from a comparable property, however, the address is still required in order to be able to identify the property, its location, size and type and any other relevant description which may influence the price. All this property information is necessary to determine the reason for the value given. The removal of a name from a comparable property, which must list the address, can still lead to the identity of a person. This may, in some circumstances, constitute a breach of the Privacy Act if this information is collected, used or disclosed without the person's permission.[32]

40.29 The REIA suggested that there already is sufficient protection to consumers under state legislation, such as the *Valuers Registration Act 1975* (NSW), to ensure that information in the hands of valuers is protected.[33] The REIA submitted:

> a. That the ALRC acknowledge that valuers are already adequately governed by State legislation which imposes professional obligations upon valuers …
>
> b. That the ALRC acknowledge that valuers protect personal and property information to the extent that names are often removed from comparable sales and leasing information contained in valuation reports unless such release is permitted by the Privacy Act.
>
> c. To enable valuers to obtain personal and property information for compiling valuation reports and for property databases, that the ALRC recommend that the Privacy Commissioner create an exemption enabling all agents to pass the required information to Valuers via a Public Interest Determination, as allowable under the Privacy Act … If there are concerns that data held by valuers may be misused, valuers can enter into a specific undertaking with the Privacy Commissioner, such as a privacy code, which will specifically regulate the collection, use and disclosure of personal information required for valuation reports and property databases.

---

30 The REIA advised that, while some real estate agencies are exempt from obligations under the NPPs due to the operation of the small business exemption, and may therefore pass information to valuers concerning recent property sales, inquiries by valuers 'have been regularly met with a refusal on the basis that it would be a breach of privacy and present the risk of complaint or prosecution': Ibid.

31 Ibid.

32 Ibid. See also Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

33 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007; Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

> d. That the ALRC recommend that the Privacy Commissioner confirm that the collection, use and disclosure of corporate sales and leasing information … is not restricted as a result of the Privacy Act and the NPPs. If this is not the case, the ALRC should recommend that the Privacy Commissioner make a Public Interest Determination to this effect.[34]

40.30 In contrast, Electronic Frontiers Australia Inc strongly opposed an exemption for valuers, and considered that individuals' names should not be disclosed to valuers without the prior explicit and informed consent of the individual concerned.[35] The OPC also opposed any such exemption.[36]

40.31 Personal information required by valuers may also be obtained from land titles offices. The REIA noted that valuers cannot rely on this information because it is 'three months to twelve months old for residential properties' and 'does not contain property descriptions necessary to determine type and size of property'.[37]

ALRC's view

40.32 In the ALRC's view, there is no compelling reason to propose an exemption or exception from *Privacy Act* obligations in relation to personal information disclosed to valuers by real estate agents, or more generally.

40.33 The Privacy Commissioner has stated that while individuals may reasonably expect that certain personal information collected by real estate agents in the course of selling a property—including the address of the property and the sale price—will be disclosed for valuation purposes, individual vendors or purchasers would not reasonably expect a real estate agent to disclose their names to valuers.[38]

40.34 The 'Use and Disclosure' principle of the proposed Uniform Privacy Principles (UPPs)—as with NPP 2.1—provides adequate latitude for the disclosure of personal information relevant to valuation. Disclosure is permitted for a related secondary purpose where the individual would reasonably expect such disclosure, or with the consent of the individual.

40.35 There is no reason to suggest that the disclosure of transaction information (address and sale price, etc) to valuers would not be within individuals' reasonable

---

34 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007. See also Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

35 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

36 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

37 Real Estate Institute of Australia, *Submission PR 84,* 12 January 2007.

38 'Privacy Legislation and It's Effect on the Valuation Industry' (2003) *Australian Property Journal* 517, 518.

expectations—given that the property market relies on the exchange of such information in order to function efficiently.[39]

40.36 Assuming that the disclosure of the name of the vendor and purchaser (if individuals) would not reasonably be expected by them, there are mechanisms that could be developed by the property industry to ensure that, where the identity of the vendor or purchaser is relevant to valuation, the relevant factors are known. For example, information about the nature of the vendor and purchaser could be developed as a set of categories used to indicate the nature of a particular sale (eg, mortgagee sale, deceased estate, owner/occupier, investor and so on).[40]

Archivists and archival organisations

40.37 In the private sector, archivists and archival organisations are responsible for the collection, maintenance and management of records that are of enduring value to individuals, organisations and businesses, and for making records available for access and research.

40.38 In a submission to the Australian Government Attorney-General's Department on the Privacy Amendment (Private Sector) Bill 2000 (Cth), the Australian Society of Archivists Inc and the Australian Council of Archives recommended an exemption for archival organisations from the operation of the NPPs to facilitate research into the administrative, corporate, cultural and intellectual activity of Australia[41]—in particular, social and genealogical research.[42]

40.39 In this Inquiry, one stakeholder submitted that 'complying with the NPPs is impossible if archives are to continue to fulfil their valuable role in society and … information privacy should not last in perpetuity'.[43]

40.40 The ALRC did not receive submissions from archival organisations expressing concern about the impact of the *Privacy Act* on their activities. The ALRC does not propose any reform in relation to exempting or excepting archivists or archival organisations from obligations under the Act.

Alternative dispute resolution bodies

40.41 An exemption from *Privacy Act* obligations has been suggested for alternative dispute resolution (ADR) bodies. In this context, ADR means dispute resolution

---

39 It is assumed that this information would be 'personal information' under the existing definition in s 6, or under the definition amended as proposed in Ch 3.

40 'Privacy Legislation and It's Effect on the Valuation Industry' (2003) *Australian Property Journal* 517, 518.

41 Australian Society of Archivists Inc, *Submission to the Federal Privacy Commissioner on the Draft National Privacy Principle Guidelines*, 2 July 2001.

42 The special arrangements in place under the *Privacy Act 1988* (Cth) to allow for the use of personal information in health and medical research, and whether these should be extended to apply to research in areas such as criminology and sociology, is discussed in Ch 58.

43 Confidential, *Submission PR 134,* 19 January 2007.

processes, other than judicial determination, in which an impartial person helps those involved in a dispute to resolve their issues.[44]

40.42 ADR schemes have been established in a number of sectors over the last 15 years, including financial services, telecommunications, and energy and water. Industry-based ADR bodies include the Telecommunications Industry Ombudsman (TIO), the Banking and Financial Services Ombudsman (BFSO) and the Financial Industry Complaints Service. These schemes have been developed in response to a need to provide an affordable and flexible alternative to the courts for consumers and small businesses seeking redress against industry sector members.[45]

40.43 In the OPC Review, a range of concerns were expressed about compliance with the NPPs by ADR bodies.[46] In response, the OPC Review recommended that the Australian Government, in recognising the important role played by ADR schemes, should consider:

- amending NPP 2 to enable use and disclosure of personal information to ADR schemes in the course of handling disputes
- amending NPP 10 to enable collection of sensitive information where it is necessary for the investigation and resolution of claims under an ADR scheme
- defining the term 'Alternative Dispute Resolution Scheme' for these purposes in the Act.[47]

40.44 In IP 31, the ALRC noted claims that organisations have refused to disclose information needed by ADR schemes to investigate claims because of a concern that disclosure would breach the NPPs.[48] The ALRC solicited views about whether legislative amendment to the privacy principles is needed to facilitate information handling by ADR bodies.[49]

---

44 See, National Alternative Dispute Resolution Council, *What is ADR?* (2007) <www.nadrac.gov.au/agd/www/Disputeresolutionhome.nsf> at 3 August 2007. The ALRC also uses the term 'external dispute resolution' (EDR) to refer to the resolution of complaints or disputes by an entity (other than a court, tribunal or government regulator) that is external to the organisation subject to the complaint or dispute, including by EDR schemes approved by the Australian Securities and Investments Commission: see Chs 45, 55.

45 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007.

46 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 231–232.

47 Ibid, 234.

48 Ibid, 232.

49 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [4.108].

40.45 In a joint submission, five industry-based ADR bodies (ADR bodies),[50] expressed concern about the impact of the NPPs on their operations. ADR schemes collect and use personal information for the purpose of resolving complaints between their members and consumers seeking redress against them ('disputants'). Obligations to comply with NPP 1 and NPP 2, however, are said to be problematic and create uncertainty.

> Unlike many other organisations that are subject to the NPPs, ADR schemes are not always able to determine in advance what information they will collect from disputants and/or members. To a large degree, disputants and members send what they consider to be relevant to the resolution of the dispute. Ultimately, the information provided may or may not be relevant to resolution of a dispute.
>
> In many cases, the member may provide information about the disputant or third parties, either because such information is contained on the relevant file, or because the member considers the information relevant to the issues in dispute, that has not been previously obtained from the disputant. Prior to the member providing the information, the disputant or third party is not in a position to advise the ADR scheme whether he or she expressly consents to the specific information being provided.[51]

40.46 Another set of concerns relates to uncertainty about whether NPP 2.1(f), which permits the disclosure of personal information in investigating or reporting 'unlawful activity' to 'relevant persons or authorities', covers disclosure to industry-based ADR schemes, such as the BFSO and TIO.

40.47 The OPC's *Information Sheet 7* states that 'self-regulatory authorities', such as the TIO and BFSO are 'relevant persons or authorities' to which an organisation may report unlawful activity.[52] Concerns remain, however, because the *Privacy Act* provides no express authority for this proposition and no assurance is provided for the use or disclosure of 'information that does not show unlawful activity but which is nevertheless necessary for the proper resolution of a dispute'.[53]

40.48 More generally, the ADR bodies noted that 'there is no express right of use or disclosure of personal information by an organisation for the purposes of asserting or defending a legal claim in a court, tribunal or other forum'. The ADR bodies submitted that, in addition to authorising use or disclosure 'required or authorised by or under law' (for example, as required by a court process):

---

50 The Banking and Financial Services Ombudsman Ltd, Energy and Water Ombudsman (Victoria), Financial Industry Complaints Service, Insurance Ombudsman Service Ltd, and the Telecommunications Industry Ombudsman.

51 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007.

52 Office of the Federal Privacy Commissioner, *Unlawful Activity and Law Enforcement*, Information Sheet 7 (2001).

53 Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007.

> NPP 2 should also include an express right for an organisation to use and disclose personal information about an individual to initiate or defend a legal or equitable claim in any court, tribunal or ADR scheme.[54]

40.49 The ADR bodies also noted that dealing with information about third parties with some connection to a dispute can be problematic—particularly in terms of the obligation to take reasonable steps to make third parties aware of collection under NPP 1.5.

> In addition, the status of ADR schemes as organisations fully subject to the NPPs can make members and others asked to provide information reluctant to do so, for fear of breaching privacy laws. Members have, on occasions, refused to provide information necessary to investigate a claim, on the basis that privacy of third parties would be breached.[55]

40.50 Finally, the collection of sensitive information about third parties was said to create problems for ADR schemes. While NPP 10 permits the collection of sensitive information about an individual if the collection is necessary for the establishment, exercise or defence of a legal or equitable claim, it is not always possible to know at the time of collection whether or not it falls into this exception.

> Many disputes brought to ADR schemes are from or about people with mental or physical illnesses. Determinations and negotiated settlements often take into consideration health information or other sensitive information about a disputant or another person. For example, where a disputant's ability to operate a bank account is affected by illness (either suffered by that person or within that person's family), such considerations are likely to be relevant to a determination and may need to be communicated to a member in order to effect a resolution to a dispute. Such information is often provided by the disputant to the ADR scheme unsolicited.[56]

40.51 In order to address these concerns about the impact of the NPPs on their operations, the ADR bodies sought the following amendments to the NPPs:

- Amendment to NPP 1 (Collection) to relieve an ADR scheme of the requirement to inform an individual of the fact of collection, where to do so would prejudice an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another person.
- Amendment to NPP 2 (Use and Disclosure) to permit the use by and disclosure to ADR schemes of personal information for the purposes of dispute resolution, regardless of whether the information is sensitive or non-sensitive in nature.

---

54 Ibid.
55 Ibid.
56 Ibid.

- Amendment to NPP 10 (Sensitive Information) to broaden paragraph 10.1(e) to permit collection of sensitive information where necessary for the investigation or resolution of a claim made to an ADR scheme.[57]

ALRC's view

40.52 The ALRC recognises that industry-based ADR schemes play an important role in the effective, efficient and fair resolution of disputes raised by Australian consumers and small businesses. The importance of this role has been recognised by their integration into the regulatory framework for a number of industry sectors.

40.53 In this Inquiry, the ALRC proposes a greater role for such schemes in the resolution of complaints about credit reporting.[58] It should be noted that, in the credit reporting context, the *Privacy Act* expressly authorises the disclosure by credit providers of personal information relating to credit worthiness:

> (i) to a person or body generally recognised and accepted in the community as being a person appointed, or a body established, for the purpose of settling disputes between credit providers, acting in their capacity as credit providers, and their customers; and
>
> (ii) for the purpose of settling a dispute between the credit provider and the individual concerned …[59]

40.54 The resolution of disputes is facilitated by the disclosure of all relevant information by the parties to dispute resolution bodies. If the *Privacy Act* presents significant barriers to the information exchange necessary for effective and efficient dispute resolution, then consideration should be given to appropriate amendment. Amendments to facilitate dispute resolution have been recommended previously by the OPC Review. The ALRC is interested in further comments on whether changes to privacy principles are desirable to address the concerns of ADR bodies.

Question 40–2 Should the *Privacy Act* or other relevant legislation be amended to provide exemptions or exceptions applicable to the operation of alternative dispute resolution (ADR) schemes? Specifically, should the proposed:

(a) 'Specific Notification' principle exempt or except ADR bodies from the requirement to inform an individual about the fact of collection of personal information, including unsolicited personal information, where to do so would prejudice an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another individual;

---

57 Ibid.
58 See Ch 55.
59 *Privacy Act 1988* (Cth) s 18N(1)(bc).

(b) 'Use and Disclosure' principle authorise the disclosure of personal and sensitive information to ADR bodies for the purpose of dispute resolution; and

(c) 'Sensitive Information' principle authorise the collection of sensitive information without consent by an ADR body where necessary for the purpose of dispute resolution?

Declared emergencies

40.55 After the release of IP 31, the *Privacy Act* was amended to insert a new Part VIA, which commenced operation on 7 December 2006.[60] The amending Act did not make any alterations to the IPPs or NPPs. Instead, Part VIA displaced some of the requirements in the IPPs and NPPs by providing a separate regime for the collection, use and disclosure of personal information where there is a connection to an emergency that has been the subject of a declaration by the Prime Minister or a minister.

40.56 In summary, Part VIA operates as follows:

- The application of Part VIA is triggered by the making of a declaration by the Prime Minister or the relevant minister, where he or she is satisfied of a number of matters, including that there has been an emergency or disaster affecting one or more Australian citizens or permanent residents.[61]

- The declaration commences when it is signed and ceases to have effect at a specified time, when revoked or after a maximum of 12 months.[62]

- When such a declaration is in force, s 80P provides that an entity (which is defined to mean an agency, organisation or other person) may, for a 'permitted purpose', collect, use or disclose personal information relating to an individual if: the entity reasonably believes the individual may be involved in the emergency or disaster; and the disclosure is to one of the persons specified.

- The term 'permitted purpose' is defined in s 80H and includes: identifying injured, missing, dead or affected individuals; assisting affected individuals in accessing services; and assisting law enforcement and coordinating the management of the situation.

---

60 *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).
61 See *Privacy Act 1988* (Cth) ss 80J, 80K, 80L.
62 Ibid ss 80M, 80N.

- Section 80Q creates an offence to disclose information obtained under Part VIA in certain circumstances, punishable by a penalty of 60 penalty units (currently $6,600) and/or imprisonment for one year.

- Division 4 of Part VIA also contains a number of technical provisions including a severability provision and a provision dealing with compensation.

40.57 The aim of the amendment was to enhance information exchange between Australian Government agencies, state and territory authorities, organisations, non-government organisations and others, in emergencies and disasters.[63] Part VIA was designed to establish a legal basis for the collection, use and disclosure of personal information about deceased, injured and missing individuals involved in an emergency or disaster.[64]

40.58 Before the *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth) was passed, a number of stakeholders expressed concern to the ALRC in relation to how the *Privacy Act* operates in emergency situations. As outlined in Chapter 22, the ALRC proposes a number of amendments to the privacy principles to cover threats to health and life and other situations—these may be referred to colloquially as emergencies, but they are not declared emergencies within the meaning of Part VIA of the Act.

40.59 A question arises, however, as to whether further refinement is desirable to the Part VIA regime.[65] A number of stakeholders have indicated that most, if not all, of the problems identified about the handling of personal information in emergency situations have been adequately dealt with by the advent of Part VIA.[66]

Background

40.60 Part VIA arose partly as a response to the concern that the provisions of the *Privacy Act* impeded the ability of agencies and organisations in responding to the emergencies of the terrorist attacks in the United States on 11 September 2001, the Bali bombings of 2002 and the Boxing Day tsunami of 2004. Given its consular obligations to assist Australians overseas in times of emergency, the Department of Foreign Affairs and Trade (DFAT) has been particularly affected in this regard. DFAT has

---

63 See Ibid s 80F; Explanatory Memorandum, Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth).

64 See Explanatory Memorandum, Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth); and P Ruddock (Attorney-General), 'Improving the Exchange of Information in Emergencies' (Press Release, 13 September 2006).

65 Some stakeholders specifically urged the ALRC to consider this question: G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

66 See, eg, Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

previously identified two key privacy impediments that hampered its response to emergencies:

> - DFAT's ability to access personal information held by other bodies to assist in its location, identification and assistance efforts; and
> - DFAT's ability to provide personal information to other bodies directly involved in the crisis response.[67]

40.61 DFAT's concern was that while it might be able, operationally, to provide personal information to other agencies directly involved in the crisis response, under IPP 11, information could not be disclosed in all cases because the disclosure could not be classified as necessary to lessen a 'serious and imminent' threat to life or health.[68] The Part VIA regime responds to this problem by not requiring an entity to establish a particular level of threat before collecting, using or disclosing personal information.

What is an 'emergency'?

40.62 The application of Part VIA is triggered by a ministerial declaration of an 'emergency'. A question arises as to whether this is the most appropriate trigger for the Part VIA regime and, if so, whether any refinements need to be made to the triggering process. Some stakeholders have expressed concern about the use of ministerial declarations as the trigger:

> Not all emergencies and disasters are declared. In many cases, [it is necessary] to start collecting and disseminating personal information before this declaration is made in order to act quickly and efficiently.[69]

Providing information to other bodies

40.63 As explained above, where there is a declared emergency, Part VIA provides a separate regime for the collection, use and disclosure of personal information that has the requisite connection to the emergency in question. This new regime was, in part, a response to a number of concerns.

40.64 First, DFAT identified an impediment regarding its ability to provide personal information to other bodies requesting the information to ensure that inappropriate action was not taken against affected Australians—for example, provision of information to Centrelink to stop it from pursuing persons affected by a disaster for overdue payments.[70] The combined effect of ss 80P(1)(c) and 80H under the Part VIA

---

67 Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

68 Ibid.

69 Confidential, *Submission PR 143,* 24 January 2007. See also Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

70 Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

regime, however, would allow DFAT and other government and non-government entities to make such a disclosure.

40.65 Secondly, concern had been expressed that under IPP 11, agencies were hampered in sharing important personal information after the immediate disaster response—that is, during the disaster recovery stage.[71] This is now dealt with in ss 80M and 80N, which provide clarity as to how long the Part VIA regime for the collection, use and disclosure of personal information will operate after a declared emergency.[72]

40.66 Other jurisdictions deal with this issue differently. For instance, Canadian law contains a broad exception to the rule against disclosure, allowing government institutions to disclose personal information for *any* purpose where, in the opinion of the head of the institution: (a) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or (b) disclosure would clearly benefit the individual to whom the information relates.[73]

Should there be an element of consent?

40.67 The NSW Council for Civil Liberties Inc suggested it might be desirable to add a mechanism for securing the consent of persons who may later be involved in an emergency overseas. It suggested the addition

> to the passenger departure form a box to tick declaring that the passenger is willing to have information released in such circumstances. This would also ensure that people who do not want their whereabouts released to indicate that.[74]

40.68 This would seem to operate as a quasi-veto, allowing individuals to state that they do not want their personal information to be shared in the event that an emergency subsequently occurs while they are outside of Australia.

ALRC's view

40.69 The ALRC has received few comments on whether Part VIA constitutes an adequate and appropriate regime for handling personal information in the context of emergencies. Given that the regime has only recently been enacted it would be premature to propose changes before there has been any opportunity to evaluate how the provisions operate in practice, in the event of a declared emergency. In view of this consideration, the ALRC does not intend to make Part VIA a particular focus of further consultation.

---

71 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

72 The Privacy Commissioner has power to give effective immunity from breaching the IPPs or NPPs in urgent situations—see *Privacy Act 1988* (Cth) pt VI, div 2.

73 *Privacy Act* RS 1985, c P-21 (Canada) s 8(2).

74 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

41. Overview—Office of the Privacy Commissioner

Contents

Introduction 1143
Consolidating functions 1144
Facilitating compliance with the *Privacy Act* 1144
Compliance-oriented regulation 1144
Enforcing compliance 1145
Structure of the OPC 1145
Regulatory structure 1145
Powers of the OPC 1146
Oversight and compliance functions 1146
Privacy codes 1146
Privacy impact assessments 1146
Investigation and resolution of privacy complaints 1147
Addressing systemic issues 1147
Framework for conciliation and determination 1147
Accountability and transparency 1147
Enforcing the *Privacy Act* 1148
Own motion investigations 1148
Strengthening the enforcement pyramid 1148
Data breach notification 1148
Proposed data breach notification provisions 1148
Summary of proposals to address systemic issues 1149

Introduction

41.1 Part F is concerned with the Office of the Privacy Commissioner (OPC). The OPC is an independent statutory body established by the *Privacy Act 1988* (Cth), consisting of the Privacy Commissioner and staff appointed under the Act. The OPC is responsible for administering the *Privacy Act*, and is the federal regulator for privacy in Australia.

41.2 General privacy regulation has operated at a federal level only since the *Privacy Act* was passed in 1988. In the early years of privacy regulation, the Privacy Commissioner was responsible for overseeing compliance with the Act by agencies and tax file number recipients. Since that time, however, the responsibilities of the

OPC have widened significantly to include credit providers, credit reporting agencies and the private sector. These changes resulted in more functions and powers for the Commissioner, although not always a commensurate increase in resources.

41.3 This chapter sets out the key themes arising out of Part F, and summarises some of the major reforms proposed by the ALRC. The chapter also examines the ALRC's approach to addressing systemic issues in privacy compliance. Before turning to those matters, however, the chapter considers the consolidation of the Commissioner's functions.

Consolidating functions

41.4 The *Privacy Act* divides the Privacy Commissioner's functions between interferences with privacy generally, tax file numbers and credit reporting. This division is a product of the historical development of the *Privacy Act*. Consistently with the ALRC's proposal that the *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity,[1] the ALRC considers that it would add greater clarity to the Act to consolidate the functions of the Commissioner where appropriate.

41.5 For example, the Privacy Commissioner's functions to investigate potential breaches of the Information Privacy Principles (IPPs), National Privacy Principles (NPPs), Tax File Number Guidelines and credit reporting provisions, could be consolidated into a general function to investigate 'interferences with privacy'. This term 'interference with privacy' is already defined to include breaches of these respective provisions. The specific functions in ss 28(1)(b)–(c) and 28A(1)(b) could then be repealed. This consolidation would be particularly appropriate if the ALRC's proposed Unified Privacy Principles (UPPs) were adopted.

41.6 Similarly, the credit reporting guidelines, advice and education functions in s 28A[2] could be rolled into their equivalent functions in s 27[3] or moved to the proposed *Privacy (Credit Reporting Information) Regulations*.[4]

Facilitating compliance with the *Privacy Act*

Compliance-oriented regulation

41.7 As the regulator responsible for administering the *Privacy Act*, the primary responsibility of the OPC is to foster and enforce compliance with the *Privacy Act*. In the Issues Paper, *Review of Privacy* (IP 31), the ALRC discussed the compliance model underpinning the *Privacy Act*—the specific modes for fostering and enforcing

1 Proposal 3–2.
2 Respectively ss 28A(1)(e), (f), and (k).
3 Those functions are *Privacy Act 1988* (Cth) s 27(1)(e), (f), and (m) respectively.
4 See Part G.

compliance, including the statutory provisions and the manner of their administration and enforcement.

41.8 Chapter 42 develops this discussion further by putting forward a model of compliance-oriented regulation as an appropriate framework in which to administer a principles-based regime such as the *Privacy Act*. Compliance-oriented regulation takes an outcomes-based approach to regulatory design, in which strategies to foster, monitor and enforce compliance with the Act are chosen 'by reference to whether they will contribute to the outcome of compliance with regulatory goals'.[5] The chapter applies the construct of compliance-oriented regulation to the *Privacy Act*, considering both the regulatory tools provided in the Act and the strategies and approaches adopted by the OPC in using those tools.

Enforcing compliance

41.9 The first elements of compliance-oriented regulation examined in Chapter 42 are securing voluntary compliance with the regulatory objectives and undertaking informed monitoring for non-compliance. The other element considered is the appropriate approach to enforcing compliance with the Act where voluntary compliance fails. The chapter sets out the benefits of adopting an explicit enforcement pyramid approach to enforcing compliance with the *Privacy Act*. This approach uses persuasive and compliance-oriented enforcement methods in the first instance, but operates in the shadow of more severe penalties where persuasive approaches fail.[6]

Structure of the OPC

Regulatory structure

41.10 Chapter 43 examines the appropriate regulatory structure for the OPC. The chapter provides an overview of the Privacy Commissioner's powers and examines the accountability mechanisms which the Commissioner is subject to under the *Privacy Act*. The ALRC proposes that the name of the OPC should be changed to the 'Australian Privacy Commission' and that the number of statutory appointees should be increased. The ALRC also proposes that the matters the Commissioner must have regard to in exercising his or her powers should be aligned with the proposed objects of the *Privacy Act*. Finally, the chapter examines the assistance given to the OPC by the Privacy Advisory Committee and proposes reform to the composition of the Committee.

---

5 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 531.

6 Ibid, 539.

Powers of the OPC

41.11 Chapter 44 examines the functions and powers vested in the Privacy Commissioner by the *Privacy Act*. The general approach of the *Privacy Act* is to state the Commissioner's 'functions' and give the Commissioner 'power' to do all things necessary or convenient to be done for or in connection with the performance of his or her functions. While much of this Discussion Paper refers to the 'OPC', the actual functions and powers outlined in the *Privacy Act* are vested in the Privacy Commissioner and are to be exercised—or delegated—by the individual appointed as Privacy Commissioner.

41.12 The Privacy Commissioner has functions in relation to interferences with privacy generally, tax file numbers and credit reporting. The Commissioner also has compliance functions under other federal legislation.

Oversight and compliance functions

41.13 Chapter 44 considers the Privacy Commissioner's functions of overseeing and monitoring compliance with the *Privacy Act*—including the functions of giving advice and guidance, undertaking educational programs, and conducting audits—and the Commissioner's powers to issue public interest determinations. The ALRC makes a number of proposals to reform these functions, to expand and strengthen the Commissioner's powers of securing and monitoring compliance with the *Privacy Act*. One proposal is to empower the Privacy Commissioner to audit an organisation's compliance with the proposed UPPs, privacy regulations, rules and any privacy code that binds the organisation.

Privacy codes

41.14 The ALRC considers the co-regulatory aspects of the *Privacy Act* in Chapter 44. These are the provisions in Part IIIAA that allow organisations to develop privacy codes, which, when approved by the OPC, replace the NPPs. The ALRC proposes that the provisions be amended so that privacy codes do not replace the proposed UPPs, but operate in addition to them, providing guidance on how one or more of the principles are to be applied or complied with by an agency or organisation. The ALRC also proposes that the Privacy Commissioner be given the power to initiate and prescribe a privacy code.

Privacy impact assessments

41.15 Chapter 44 also examines the very topical issue of privacy impact assessments. The chapter looks at the role of privacy impact assessments in the regulatory regime, and considers the role they play in facilitating privacy compliance. The ALRC proposes that the *Privacy Act* be amended to empower the Privacy Commissioner to direct an agency or organisation to provide to the Commissioner a privacy impact assessment in relation to a new project or development that the Commissioner considers may have a significant impact on the handling of personal information.

Investigation and resolution of privacy complaints

41.16 Concern has been expressed by stakeholders about the current complaint-handling process in the *Privacy Act*. In Chapter 45, the ALRC proposes to reform the existing provisions to streamline, and increase the effectiveness of, complaint handling under the Act.

Addressing systemic issues

41.17 Stakeholders expressed concern about the ability of the OPC to address systemic issues in privacy compliance. By systemic issues, the ALRC is referring to 'issues that are about an organisation's or industry's practice rather than about an isolated incident'.[7]

41.18 To facilitate a shift in focus to systemic issues, the ALRC proposes that the OPC be devolved of some of the responsibility for handling privacy complaints under the Act. Some privacy complaints, particularly in the credit reporting area, could instead by handled by external dispute resolution schemes. The ALRC proposes that the Privacy Commissioner be given a specific decline and referral power for these purposes.

41.19 The ALRC also proposes that the Privacy Commissioner's power to remedy systemic issues be enhanced by empowering the Commissioner to prescribe, in a determination, the steps an agency or organisation must take to comply with the *Privacy Act*.

Framework for conciliation and determination

41.20 The second central issue examined in Chapter 45 is the manner in which complaints are resolved under the *Privacy Act*. The ALRC proposes that the Act be amended to include a new framework to deal with conciliation and determination. This framework would, amongst other things, give complainants and respondents the right, in certain circumstances, to require the Commissioner to resolve a complaint by determination.

Accountability and transparency

41.21 Chapter 45 also considers issues of accountability and transparency in handling privacy complaints. The ALRC proposes that the *Privacy Act* be amended to provide merits review of all determinations made by the Privacy Commissioner and that the OPC publish a document setting out its complaint-handling policies and procedures.

---

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 130 fn 102.

Enforcing the *Privacy Act*

Own motion investigations

41.22 Chapter 46 examines the OPC's powers to enforce compliance with the *Privacy Act*. The chapter focuses on the Privacy Commissioner's powers to commence on the Commissioner's own motion an investigation into an act or practice that may be an interference with privacy. This own motion investigation power complements the Commissioner's power under the *Privacy Act* to investigate complaints. A significant limitation on the Commissioner's own motion investigation powers, however, is the inability to prescribe or enforce remedies where the Commissioner finds that an agency or organisation has contravened the privacy principles. The ALRC proposes that the Privacy Commissioner be empowered to impose remedies where he or she finds a breach of the principles following an own motion investigation.

Strengthening the enforcement pyramid

41.23 Chapter 46 also considers the question whether there needs to be further remedies or penalties available under the Act to enforce compliance. Taking into account the enforcement pyramid approach discussed in Chapter 42, the ALRC proposes that civil penalties be introduced for serious or repeated interferences with the privacy of an individual. This proposal is intended to strengthen the overall enforcement pyramid underpinning the *Privacy Act*, and should provide strong incentives for increased compliance by agencies and organisations.

Data breach notification

41.24 Chapter 47 examines data breach notification. The security of personal information is a growing concern in privacy regulation around the world. One regulatory response to the increasing number of data breaches has been to require agencies or organisations to notify individuals affected where there has been an unauthorised acquisition of personal information.

41.25 In Chapter 47, the ALRC considers the rationale behind mandatory reporting of data breaches, and examines some of the models for data breach notification laws. The key issues considered are the triggering event, the general exceptions to notification and the scope of the responsibility to notify.

Proposed data breach notification provisions

41.26 In the ALRC's view, there is a strong regulatory justification for introducing a requirement for agencies and organisations to report data breaches to individuals affected and to the OPC. The ALRC puts forward a model where notification would be required if specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or the Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual. Exceptions to this requirement would be where

the personal information is adequately encrypted, where the breach was internal and there was no further disclosure, or where the Privacy Commissioner does not consider that notification would be in the public interest. To provide strong incentives for compliance with the proposed data breach notification provisions, the ALRC proposes that failure to notify the Commissioner of a data breach attract a civil penalty.

Summary of proposals to address systemic issues

41.27 As noted above, a major concern of stakeholders is the ability of the OPC to address systemic issues. In the ALRC's view, the OPC requires a number of tools and strategies to enable it to discover, monitor and remedy systemic issues in agencies, organisations and industries. Ideally, these tools and strategies must allow the Privacy Commissioner to act proactively to identify and resolve systemic issues before a breach occurs and, when enforcing the Act, to act in a manner which will provide specific deterrence to the agency or organisation involved and general deterrence to other agencies and organisations.

41.28 The ALRC puts forward a number of proposals throughout Part F that are aimed at increasing the OPC's ability to monitor and remedy systemic issues. Taken as a whole, the ALRC believes that these proposals would provide the OPC with an appropriate 'toolkit' to deal with systemic issues in privacy compliance.[8]

8 See Proposals 44–6, 44–9, 44–10, 45–2, 45–5, 45–6, 46–1, 46–2.

Part F

Office of the Privacy Commissioner

42. Facilitating Compliance with the *Privacy Act*

Contents

Introduction 1151
Compliance-oriented approach to privacy regulation 1152
Principles-based regulation 1152
Elements of compliance-oriented regulation 1152
Securing compliance 1153
Monitoring compliance 1154
Enforcing compliance 1155
Submissions and consultations 1157
ALRC's view 1157

Introduction

42.1 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the current compliance model used in the *Privacy Act 1988* (Cth) is appropriate and effective to achieve the Act's purposes, and if not, whether that is because of its content, its administration, or some other reason.[1] By 'compliance model', the ALRC is referring to the specific modes for fostering and enforcing compliance, including the statutory provisions and the manner of their administration and enforcement.

42.2 In this chapter, the ALRC considers what would be the appropriate compliance model to adopt in regulating privacy in Australia. This chapter is primarily descriptive and analytical, and does not contain any proposals for reform. It aims to provide a theoretical framework that will help in considering the ALRC's proposals to expand the functions and powers of the privacy regulator in Australia to facilitate compliance with the *Privacy Act*.[2]

1 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–21.
2 These proposals are set out in Chs 44–46.

Compliance-oriented approach to privacy regulation

Principles-based regulation

42.3 The *Privacy Act* adopts a principles-based approach to regulating privacy. As explained in Chapter 15, principles-based regulation relies on high level, broadly stated standards or principles, rather than 'bright-line' or detailed, prescriptive rules.[3]

42.4 The guiding purpose of a principles-based approach is to shift the regulatory focus from process to outcomes. It is based on the idea that the agency or organisation itself is 'better placed than regulators to determine what processes and actions are required within their businesses to achieve a given regulatory objective'.[4] Regulators should focus on defining the outcomes they want regulated entities to achieve—for example, by using a principle to set a high-level objective—instead of focusing on prescribing the processes or actions the entities must take. This leaves the regulated entity 'free to find the most efficient way to achieving the outcome required'.[5]

Elements of compliance-oriented regulation

42.5 Compliance-oriented regulation adopts 'an outcomes-based approach to total regulatory design'.[6] Compliance-oriented regulation is 'a total package in which all the factors of regulatory rule making, monitoring, and enforcement are designed to elicit a particular regulatory objective'.[7] Dr Christine Parker has identified a number of elements of compliance-oriented regulation, which can be grouped into: securing voluntary compliance with the regulatory objectives; undertaking informed monitoring for non-compliance; and engaging in enforcement actions where voluntary compliance fails.[8]

42.6 The ALRC considers that compliance-oriented regulation can provide the framework for a principles-based regime such as the *Privacy Act*. The theory on which compliance-oriented regulation is based provides a prism through which to view and assess the compliance model underpinning the *Privacy Act* and the approach taken by the Office of the Privacy Commissioner (OPC) to fostering compliance. It also provides an holistic approach for considering which regulatory strategies would best achieve the objectives of the *Privacy Act*.[9]

---

3 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 3.

4 Ibid, 5.

5 Ibid, 5. See also C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 547.

6 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 531.

7 Ibid, 535.

8 Ibid, 535.

9 Ibid, 531.

42.7 In this chapter, the ALRC draws on the work of Parker on compliance-oriented regulation as a useful model to apply to the privacy context. Parker has conducted extensive empirical research and published widely on corporate compliance and regulatory enforcement strategies. The chapter considers the elements of compliance-oriented regulation identified by Parker and applies them to the privacy context, focusing on the regulatory tools provided in the *Privacy Act* and the strategies and approaches adopted by the regulator in using those tools. It then considers how these current provisions or practices can be improved to facilitate compliance with the Act.

Securing compliance

42.8 Parker explains that the first step of compliance-oriented regulation is 'providing incentives and encouragement to voluntary compliance and nurturing the ability for private actors to secure compliance through self-regulation, internal management systems, and market mechanisms where possible'.[10] A key way a regulator can help foster an agency's or organisation's capacity to comply is through education and other assistance.[11]

42.9 This first step of compliance-oriented regulation is reflected in the OPC approach to promoting compliance with the *Privacy Act*, which is based on the premise that 'compliance will be achieved most often by helping organisations to comply rather than seeking out and punishing the few organisations that do not'.[12] The OPC has stated that its 'first and preferred approach at all times' will be on providing advice, assistance and information.[13] The Act provides the Privacy Commissioner with an array of tools to provide this assistance, including specific functions of giving advice, undertaking education programs and issuing guidelines to help agencies and organisations comply with the privacy principles and the objects underlying these principles. Co-regulation is also provided for in the Act, by allowing organisations to develop specialised codes for the handling of personal information which, when approved by the OPC, replace the privacy principles.[14]

42.10 While fostering compliance through providing advice, encouragement and guidance to agencies and organisations is consistent with compliance-oriented regulation, a proliferation of guidance can undermine the administration of a principles-based regime, as it can increase prescription, complexity and inaccessibility.[15] It can also deprive the regulator of the benefits of a principles-based

---

10 Ibid, 539.
11 Ibid, 554.
12 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 1.
13 Ibid, 1.
14 *Privacy Act 1988* (Cth) s 16A.
15 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 15–16.

approach by 'creating expectations as to its own conduct in the future'. That is, while the regulator may see guidance as advisory only, the regulated entities may understand it as being the definitive interpretation of the principles.[16] The OPC should have regard to this tension in administering the principles-based regime of the *Privacy Act*.

42.11 Another technique suggested by Parker to foster compliance is to encourage the growth of 'compliance professionals'—individuals with specialist expertise who provide advice on how to comply with particular laws.[17] On this point, the ALRC notes the emergence of the 'privacy professional' in recent years, and the increasing profile of 'privacy officers' in the organisational hierarchy.[18] The OPC should continue to encourage the growth of this privacy profession—including through networks such as the privacy contact officer network—to help build compliance into organisational practice and develop a shared understanding of the objectives of the *Privacy Act*.[19]

Monitoring compliance

42.12 The second element of compliance-oriented regulation is 'informed monitoring for non-compliance'.[20] Monitoring must be used 'to determine whether regulatory design is having its desired effect on the target population'.[21] As regulators cannot enforce every rule or cover every problem, they should use information collected about the regulatory problem to develop a 'risk-based approach to targeting inspections'.[22] Monitoring can be used as a proactive tool to secure compliance in the first instance and to ensure that compliance has been restored after an incident of non-compliance.

42.13 The *Privacy Act* already provides the Privacy Commissioner with a number of ways to monitor compliance with certain provisions of the Act by agencies and organisations.[23] The Privacy Commissioner's powers to audit organisations for compliance with the National Privacy Principles is more limited, however, and can only be done on request by the organisation. To extend the Commissioner's power to determine whether regulatory objectives are being achieved in organisations as well as

16 Ibid, 16.
17 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 554.
18 The growing prominence of privacy officers within corporations was noted in International Association of Privacy Professionals, 'Ponemon Institute, IAPP Announce Results of Annual Salary Survey' (Press Release, 11 March 2005).
19 The ALRC notes the OPC Review's recommendation that it would 'develop strategies for communication with stakeholders, including establishing a privacy contact officer network for private sector organisations': see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 50.
20 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 535.
21 Ibid, 537.
22 Ibid, 537.
23 See *Privacy Act 1988* (Cth) ss 27(1)(h)–(ha), 28(1)(e), 28(1)(h), 28A(1)(g)–(j).

agencies, the ALRC proposes that the *Privacy Act* be amended to give the Commissioner a 'spot audit' power over organisations.[24]

Enforcing compliance

42.14 A compliance-oriented regulatory design also must provide for enforcement in the event of non-compliance. Parker explains that in compliance-oriented regulation, when organisations fail to comply in the first instance, the preferred approach would be to 'attempt to restore or nurture compliance rather than reverting immediately to a purely punishment-oriented approach'.[25] These attempts to restore compliance, however, must operate in the presence of more punitive sanctions, as the evidence shows that 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.[26]

> The idea is that regulators should engage tit for tat in restorative or persuasive enforcement strategies depending on the responses of the regulated entity. A regulator can start with persuasive or restorative strategies and then move to more punitive strategies if voluntary compliance fails. If the application of punitive sanctions succeeds in bringing about compliance, then the regulator can revert to a trusting demeanour. If it does not bring about compliance, then the regulator must invoke harsher sanctions. The wider the range of strategies (from restorative to punitive) available to the regulator, the more successful tit-for-tat enforcement is likely to be.[27]

42.15 This principle is encapsulated in Professors Ian Ayres and John Braithwaite's enforcement pyramid.[28] Braithwaite contends that compliance is 'most likely' when a regulator displays an explicit enforcement pyramid:

> Most regulatory action occurs at the base of the pyramid where initially attempts are made to coax compliance by persuasion. The next phase of enforcement escalation is a warning letter; if this fails to secure compliance, civil monetary penalties are imposed; if this fails, criminal prosecution ensues; if this fails, the plant is shut down or a licence to operate is suspended; if this fails, the licence to do business is revoked. The form of the enforcement pyramid is the subject of the theory, not the content of the particular pyramid.[29]

---

24 See Proposal 44–6.

25 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 539.

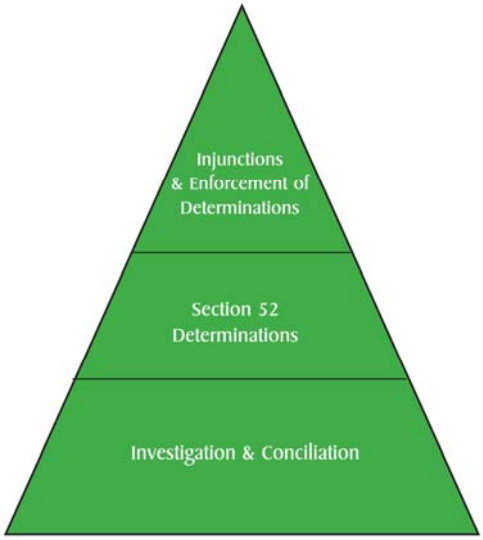
26 Ibid, 541. See also J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science.

27 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 541.

28 The model was first put forward by Braithwaite in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985). See also B Fisse and J Braithwaite, *Corporations, Crime and Accountability* (1993); C Dellit and B Fisse, 'Civil and Criminal Liability Under Australian Securities Regulation; The Possibility of Strategic Enforcement' in G Walker and B Fisse (eds), *Securities Regulation in Australia and New Zealand* (1994), 570.

29 Quoted in F Haines, *Corporate Regulation: Beyond 'Punish or Persuade'* (1997), 218–219.

42.16 There is a level of escalation involved in the approach taken to resolving privacy complaints and taking other enforcement action under the *Privacy Act*. This is illustrated in the following diagram.



42.17 As this pyramid demonstrates, coaxing compliance occurs through undertaking investigations and conciliating complaints about interferences with privacy. The next level up is for the Privacy Commissioner to make determinations under s 52, which can involve an element of sanction via a public declaration of breach. The Commissioner can also enforce its own determinations in the federal courts and apply for injunctions.

42.18 This escalation of sanctions has not always been reflected, however, in the OPC's approach to enforcement. In the OPC Review, the OPC acknowledged that it had 'made limited or no use of the more formal enforcement powers, such as making complaint determinations or seeking injunctions from the court, or publicly "naming" and "shaming"'.[30] The OPC explained that this was in part due to: its strong focus on conciliation in resolving individual complaints; the fact that injunctions are more likely to be relevant where there is significant and immediate harm and the respondent is recalcitrant; and the fact that the OPC has received a generally good level of cooperation when it pursues issues.

30 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 126. See also Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001).

42.19 Nevertheless, the OPC Review acknowledged the concern expressed by some consumers and privacy advocates that the enforcement of the *Privacy Act* is 'soft'.[31] It recommended that, while it would maintain its current approach to compliance, it would consider whether it might be appropriate in some circumstances to use its other powers earlier, such as the determination power.[32]

Submissions and consultations

42.20 Several stakeholders commented on the enforcement approach adopted in the *Privacy Act* and by the OPC. Some stakeholders supported the OPC's current approach to compliance and the compliance model in the *Privacy Act*.[33] Stakeholders also expressed support for the use of Braithwaite's 'enforcement pyramid' as a model for enforcing the *Privacy Act*.[34] The OPC suggested that the Act be amended to include stronger powers to handle systemic issues and issues arising from industry practice.[35]

42.21 Other stakeholders suggested better use could be made of the Privacy Commissioner's functions and powers to enhance the OPC's approach to compliance.[36] The Consumer Credit Legal Centre (NSW) (CCLC) found that, in its experience, there is 'no culture of compliance and there is little incentive for respondents to complaints to correct systemic flaws'.[37] The CCLC submitted that the OPC's current approach to compliance is ineffective and strongly supported the consideration of other schemes that contain stronger penalties.

ALRC's view

42.22 The ALRC makes several proposals in Chapters 45 and 46 that are aimed at strengthening the restorative elements of complaint-handling under the Act and enhancing the enforcement pyramid adopted in the *Privacy Act,* by expanding the remedies and sanctions available to the Privacy Commissioner when he or she finds an interference with privacy. The ALRC also proposes that the content of the enforcement

---

31 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 152. See also S Hayes, 'Privacy Boss Tips Soft Option', *The Australian* (Sydney), 3 August 2004, 29.

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 37. See also rec 42.

33 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007. See also Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

34 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007.

35 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

36 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

37 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

pyramid adopted in the *Privacy Act* be strengthened with the addition of civil penalties for serious or repeated contraventions of the Act.

42.23 These proposals are consistent with Parker's model and aim to widen the range of strategies that are available to the OPC to enforce compliance with the *Privacy Act*. It is important, however, that the OPC adopt a compliance-oriented approach in applying these strategies. While it is consistent with compliance-oriented regulation to focus initially on restoring compliance through negotiated outcomes (such as conciliation), the OPC should not confine itself to this approach. In particular, the ALRC notes Parker's suggestion that a compliance-oriented regulatory design must incorporate enforcement, 'otherwise, regulators cannot meaningfully and discriminately apply incentives, persuasion, and cooperation to organisations that are complying or attempting in good faith to comply'.[38]

42.24 It is crucial that there be an element of public enforcement in the OPC's regulation of privacy, consistent with Parliament's expectation that the Commissioner 'be the means by which there will be accountability to the public on the use by government of their personal information'.[39] A clear enforcement policy that outlines what the usual response to a particular type of breach will be and how that response can be mitigated—such as by evidence of a good internal compliance program—can provide incentives for organisations to put in place those mitigating practices. Such a policy also allows the regulator to discriminate between agencies and organisations that are genuinely trying to comply and those that are not. The regulator can then adopt enforcement responses that send a strong message of general deterrence to the regulated community. This encourages agencies and organisations to keep complying (or at least keep trying to comply), as they will see that non-compliance, combined with no effort to comply, will attract strong sanctions from the regulator.

42.25 Consistent with the compliance-oriented regulatory design underpinning the *Privacy Act*, the OPC should implement a compliance policy that adopts an explicit enforcement pyramid approach to restoring compliance and enforcing the *Privacy Act*. The OPC should use, and should be seen to be using, a wide range of strategies to ensure compliance with the *Privacy Act*, recognising the benefits of specific and general deterrence that can be generated by a transparent, balanced and vigorous enforcement approach.

---

38 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 534.

39 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). This speech only refers to the government, as organisations were not covered by the *Privacy Act* when the Act was originally passed.

43. Structure of the Office of the Privacy Commissioner

Contents

Introduction 1160
Structure, functions and powers 1160
- Legislative structure 1160
- Functions and powers of the OPC 1161
- Delegation 1161
- Regulatory structure 1162
- Submissions and consultations 1163
- ALRC's view 1164

Manner of exercise of powers 1166
- Section 29 of the Privacy Act 1166
- Submissions and consultations 1167
- ALRC's view 1168

Accountability mechanisms 1169
- Judicial review 1169
- Merits review 1170
- Commonwealth Ombudsman 1170
- Submissions and consultations 1171
- ALRC's view 1171

Criminal liability 1172
- Background 1172
- Submissions and consultations 1172
- ALRC's view 1172

Immunity 1172
- Background 1172
- Submissions and consultations 1173
- ALRC's view 1174

Privacy Advisory Committee 1175
- Composition 1175
- Functions 1176
- Submissions and consultations 1177
- Options for reform 1180
- ALRC's view 1180

Introduction

43.1 This chapter considers the structure of the Office of the Privacy Commissioner (OPC). The discussion focuses on the existing structure, functions and powers of the Privacy Commissioner, the constraints on the exercise of the Commissioner's powers, the liabilities to which the Commissioner is subject and the immunities the Commissioner enjoys. The chapter also considers the Privacy Advisory Committee, including its composition and functions.

43.2 The ALRC will make a number of proposals in this chapter, which, if implemented, will result in an updating of the legislative structure of the OPC. The ALRC proposes that the name of the OPC be changed to the Australian Privacy Commission and the number of statutory appointees to the Commission be increased. The ALRC also makes the proposal to align the matters that the Commissioner must have regard to in performing functions and exercising powers with the proposed objects of the *Privacy Act 1988* (Cth). This chapter includes a number of proposals relating to the Privacy Advisory Committee, including a proposal that the membership criteria for the Committee be updated and extended. The chapter also includes a proposal that the Act empower the Commissioner to draw on the assistance of expert panels.

Structure, functions and powers

Legislative structure

43.3 The role and position of Privacy Commissioner was originally established in the *Privacy Act*, as passed in 1988. The Commissioner was initially a member of the Human Rights and Equal Opportunity Commission (HREOC), before the OPC was established as a separate office in July 2000. It was suggested that a separate office was consistent with the approach taken in other countries and that it would provide 'an opportunity to further increase the profile, and thus the effectiveness, of the work of the Privacy Commissioner and of the office of the Privacy Commissioner'.[1]

43.4 The *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth) amended the *Privacy Act* to establish the 'Office of the Privacy Commissioner', defined to consist of the Privacy Commissioner and staff appointed under s 26A.[2] The *Privacy Act* provides that the Commissioner is appointed by the Governor-General for a period of up to seven years,[3] on such terms and conditions as imposed by the Governor-General and the Act.[4] The Commissioner's appointment may be terminated

1 Commonwealth, *Parliamentary Debates*, House of Representatives, 9 December 1998, 1660 (D Williams—Attorney-General), 1660.
2 *Privacy Act 1988* (Cth) s 19.
3 Ibid ss 19A(1), 20(1).
4 Ibid s 20.

because of misbehaviour, or physical or mental incapacity, and must be terminated in circumstances of bankruptcy, extended absence or unapproved outside employment.[5]

43.5 The *Privacy Act* does not provide for a Deputy or Assistant Commissioner (as a statutory appointee), but does provide for the appointment of an Acting Commissioner during any vacancy in the office or absence of the Privacy Commissioner.[6] Although this is similar to the approach taken in Australian states, both Canada and New Zealand provide for the appointment of additional statutory officers. For instance, in New Zealand, the Governor-General may, on the recommendation of the Minister, appoint a Deputy Commissioner, who is entitled to all the protections, privileges and immunities of the Commissioner and, subject to the control of the Commissioner, has and may exercise all the powers, duties and functions of the Commissioner under the Act.[7]

Functions and powers of the OPC

43.6 Part IV, Division 2 of the *Privacy Act* vests a range of functions in the Commissioner. These functions are examined in Chapters 44–46 and are divided in the Act into functions relating to interferences with privacy, tax file numbers, and credit reporting.[8] The Privacy Commissioner also has functions under other Acts, which are examined further in Chapter 44 and Part J.

43.7 The *Privacy Act* invests the Commissioner with power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions.[9] The Commissioner also has an ancillary function in s 27(1)(s) to do anything incidental or conducive to the performance of any of the Commissioner's other functions in s 27(1).[10]

Delegation

43.8 There are two matters to note about the Commissioner's legislative functions and powers. The first is that the *Privacy Act* invests functions in the Privacy Commissioner personally, rather than in the OPC generally, and only the Commissioner has the power to do all things necessary or convenient to be done in connection with the performance of his or her functions.

---

5 Ibid s 25.

6 Ibid s 26.

7 *Privacy Act 1993* (NZ) s 15. In addition, in Canada the Governor in Council may, on the recommendation of the Privacy Commissioner, appoint one or more Assistant Privacy Commissioners, who engage exclusively in duties or functions of the office of the Privacy Commissioner as delegated by the Privacy Commissioner: *Privacy Act* RS 1985, c P-21 (Canada) s 57.

8 The Commissioner's functions and powers in relation to general interferences with privacy are set out in detail in Ch 44. The Commissioner's functions in relation to credit reporting are discussed in Part G.

9 *Privacy Act 1988* (Cth) ss 27(2), 28(2), 28A(2).

10 Ibid s 34 limits the Commissioner's powers 'in connection with the performance of the functions referred to in section 27' in relation to documents exempt under the *Freedom of Information Act 1982* (Cth).

43.9 Secondly, the Privacy Commissioner can delegate all or any of his or her powers either to a member of the Commissioner's staff or a member of the staff of the Commonwealth Ombudsman, with two exceptions. The Commissioner cannot delegate the powers conferred by s 52, which sets out the Commissioner's power to make determinations, and the Commissioner cannot delegate his or her power under s 17 to issue guidelines relating to tax file number information.[11]

Regulatory structure

43.10 The Privacy Commissioner, supported by the OPC, is an individual, independent regulator, rather than a regulatory agency or commission.[12] There has been some discussion by regulatory theorists about the distinction between an independent individual regulator, such as the Privacy Commissioner, and a commission-style regulator. It has been noted that the rationale for attaching regulatory powers to an individual is

> 'to seek to develop a quicker and less bureaucratic system of regulation. This was centred on the idea of a single, independent regulator for each industry, operating without undue bureaucracy and supported by a small staff.' It was considered, further, that personal responsibility for regulation would reassure the public who could identify regulation with an individual protector of their interests rather than some vague commission of faceless persons.[13]

43.11 The disadvantages of an individual regulator include: the possibility that significant political pressures may be directed at one person; a lack of accountability to a board or equivalent; and the potential for unpredictable decision making.[14] An individual regulator structure means 'important decision making functions which are material to the rights and privileges of third parties' are vested in one individual, which could result in one individual being responsible for advising organisations and adjudicating disputes involving the same organisation.[15] This can raise the danger that the regulator will, or will be seen to, 'fall between stools' such that its enforcement actions are seen as tainted by its policy-making concerns, and vice versa.[16]

43.12 An alternative structure to an individual regulator is a commission. Proponents of commissions argue that a commission structure: helps reduce the danger that regulators will feel vulnerable and behave defensively; creates a sense that decisions follow internal debate; increases legitimacy and accountability; and spreads the

---

11 *Privacy Act 1988* (Cth) s 99.

12 Note that s 26A of the *Privacy Act* provides that the Commissioner and the Australian Public Service employees assisting the Commissioner constitute a Statutory Agency for the purposes of the *Public Service Act 1999* (Cth) and the Commissioner is the Head of the Statutory Agency.

13 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 71: quoting United Kingdom Government National Audit Office, *The Work of the Directors General of Telecommunication, Gas Supply, Water Services and Electricity Supply* (2006), [2.3].

14 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 324.

15 United Kingdom Director General of Telecommunications, *Submission to the Review of Utility Regulation*, 1 September 1997, [5.31].

16 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 70–71.

workload involved in regulating complex industries.[17] Critics, however, argue that a commission structure may lead to: inconsistent decisions, as decisions would be made by a commission whose composition may change; slower decision making; and possible loss of clarity of responsibility.[18]

Submissions and consultations

43.13 The ALRC asked in Issues Paper 31, *Review of Privacy* (IP 31) whether the legislative structure of the OPC is appropriately meeting the needs of the community.[19] Several submissions received by the ALRC suggested there was no reason to alter the legislative structure of the OPC.[20] The OPC itself supported the continuation of the OPC as a statutory body with a Commissioner appointed for a specified term, noting that it was consistent with international standards regarding privacy regulation.[21]

43.14 In contrast, the Australian Privacy Foundation (APF) suggested that, while the OPC is performing many valuable functions, it 'is not currently meeting the legitimate expectations of the community, either in relation to complaint handling or in relation to wider roles of advocacy and pro-active enforcement'. The APF suggested, however, that it was difficult to identify whether this overall failing is due to the structure of the Act as opposed to the exercise of the functions by successive Commissioners.[22]

43.15 In terms of the name of the regulator, the OPC reiterated the recommendation made in its review of the private sector provisions of the *Privacy Act* (OPC Review) that its name should be changed to the 'Australian Privacy Commission'.[23] The OPC argued that the similarity of names between state privacy regulators and the OPC causes confusion for consumers who are trying to work out to whom they should make a complaint. The OPC also argued that renaming the office as suggested would be more consistent with other federal regulators, such as the 'Australian Competition and Consumer Commission' and the 'Australian Securities and Investments Commission'.[24] The Australian Government did not rule out the name change in its

17 Ibid, 324.
18 Ibid, 324–325.
19 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–1.
20 See G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.
21 See the *Criteria and Rules for Credentials Committee and the Accreditation Principles*, (Adopted on 25 September 2001 during the 23rd International Conference of Data Protection Commissioners held in Paris, 24–26 September 2001 and as amended on 9 September 2002 during the 24th International Conference of Data Protection and Privacy Commissioners held in Cardiff 9–11 September 2002).
22 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
23 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 6.
24 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 47.

response to the OPC Review, but rather noted that it would give further consideration to the issue, including any costs associated with the change.[25]

43.16 The OPC also commented on the delegation power in its submission, recommending that the exception in the Commissioner's powers to delegate with regard to s 52 determinations be amended to allow senior staff of the OPC to undertake determinations. In making this suggestion, the OPC acknowledged that the determinations power is a significant power and the limitation of its exercise to the Commissioner, as an independent statutory officer, is reflective of this significance.[26] Without the power to delegate the determinations power, however, the OPC noted that its exercise is necessarily limited to the individual Commissioner's availability. In light of the Commissioner's recent commitment to undertake more determinations,[27] the OPC suggested that it would be preferable, and may become necessary, for the determinations power to be exercisable by other senior staff members (such as the Deputy or Assistant Commissioner). The OPC suggested that this could be done by either introducing a qualified delegation power in respect of the Commissioner's determination powers or by amending the *Privacy Act* to specify an additional position or positions that would be permitted to exercise the determinations power.[28]

ALRC's view

43.17 The legislative structure of the OPC is an integral part of building an effective infrastructure for privacy regulation in Australia. It is critical that the body responsible for regulating the personal information-handling practices of the federal public sector and applicable organisations is structured and constituted in a manner that best helps it achieve its legislative purpose to promote and protect privacy in Australia.[29]

43.18 The ALRC's view is that the following steps need to be taken: the OPC should be renamed the 'Australian Privacy Commission'; and the number of statutory appointments to the Office should be expanded. To this end, the *Privacy Act* should be amended to allow for the appointment of one or more Deputy Privacy Commissioners. The Deputy Commissioners would be appointed by the Governor-General under the *Privacy Act* for a set period and would enjoy the same level of independence, including through the protections against termination of appointment that currently apply to the

---

25 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), [Number 6].

26 See also Australian Public Service Commission, *Foundations of Governance in the Australian Public Service* (2005), 31.

27 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 37, 42; Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2.

28 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. The OPC noted that while it had not identified a similar problem in respect of the limitation on delegating its powers in relation to Tax File Number Guidelines, there was also no strong reason why the power should not also be delegable, particularly as the Guidelines are disallowable instruments.

29 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 30 July 2007.

Privacy Commissioner.[30] The Deputy Privacy Commissioners should be empowered to exercise all the powers, duties and functions of the Commissioner under the Act—including the powers in ss 52 and 28A(1)(a)—subject to the oversight of the Privacy Commissioner.

43.19 The ALRC's view is that increasing the size of the OPC should facilitate more accountability and transparency in its operations and encourage more formal, collegiate decision making. This should help respond to concerns raised by stakeholders over the lack of transparency and accountability in the OPC's processes and procedures, particularly in relation to complaint handling, the issues of delay in the Office's investigation and conciliation processes, and the limited exercise of the determinations power in s 52.[31]

43.20 Increasing the number of statutory appointees would also provide a means to address the delegation issue raised by the OPC. The ALRC's view is that the determination power is significant and should only be exercised by statutory officers appointed under *Privacy Act*. Although—following the High Court's decision in *Brandy v Human Rights and Equal Opportunity Commission*,[32]—determinations are no longer binding and conclusive between parties, the power to issue determinations is still one of the most significant powers vested in the Commissioner. The proposal to appoint more statutory officers who are expressly authorised to exercise all the powers of the Privacy Commissioner—including a power under s 52—respects the significance of the power in s 52 and ameliorates the problem of it being limited to one person's availability. Having additional statutory officers with power to make determinations should also give the OPC the means to address concerns about the rare use of the determinations power and would facilitate implementation of the ALRC's proposal to give complainants and respondents the right in certain circumstances to require the Commissioner to issue a determination in relation to their complaint.[33]

43.21 Finally, expanding the OPC to include at least two statutory officers (with potential for more) provides additional support for changing the name of the OPC to the Australian Privacy Commission. This is because a body constituted by multiple statutory officers is consistent with the general understanding of a commission as a body of persons charged with particular functions, rather than an individual regulator.

---

30 That is, as set out in s 25 of the *Privacy Act 1988* (Cth).

31 These concerns were raised by a number of stakeholders and are discussed in detail in Ch 45.

32 *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245. Following *Brandy*, the *Human Rights Legislation Amendment Act 1995* (Cth) removed the Commissioner's power to register determinations in the Federal Court.

33 Proposal 45–5.

Proposal 43–1 The *Privacy Act* should be amended to change the name of the 'Office of the Privacy Commissioner' to the 'Australian Privacy Commission'.

Proposal 43–2 Part IV, Division 1 of the *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioners may exercise all the powers, duties and functions of the Privacy Commissioner under this Act—including a power conferred by s 52 and a power in connection with the performance of the function of the Privacy Commissioner set out in s 28(1)(a)—or any other enactment.

Manner of exercise of powers

Section 29 of the Privacy Act

43.22 In exercising his or her powers under the *Privacy Act*, the Commissioner is bound to have regard to the matters set out in s 29. The matters in s 29 can be divided into two principal concerns. First, the *Privacy Act* requires the Commissioner to take the following into account when performing functions and exercising a power:

- protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the recognition of the right of government and business to achieve their objectives in an efficient way;[34] and

- international obligations accepted by Australia, including those concerning the international technology of communications, and developing general international guidelines relevant to the better protection of individual privacy.[35]

43.23 Secondly, the *Privacy Act* requires the Commissioner to ensure that his or her recommendations, directions and guidelines are capable of being accepted, adapted and extended throughout Australia,[36] and are consistent with whichever is relevant out of the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs), *Credit Reporting Code of Conduct* and Part IIIA of the Act.[37]

43.24 The Explanatory Memorandum to the Privacy Bill 1988 (Cth) explained that s 29 requires the Commissioner 'to balance the need to ensure proper protection from

34 *Privacy Act 1988* (Cth) s 29(a).
35 Ibid s 29(b).
36 Ibid s 29(c).
37 Ibid s 29(d).

interferences of privacy against the requirements of government and private sector bodies to achieve their objectives in an efficient manner'.[38] The OPC has previously explained that 'the legislation acknowledges that privacy is not an absolute right and that an individual's right to protect his or her privacy must be balanced against a range of other community and business interests'.[39]

43.25 The New Zealand *Privacy Act* requires its Privacy Commissioner to have regard to largely the same matters as set out in s 29.[40] In other jurisdictions, an alternative approach is taken. Instead of explicitly requiring the privacy regulator to have regard to certain matters in the exercise of their powers, the privacy legislation acknowledges matters such as the competing interests of human rights and organisational efficiency in the preamble or objects section.[41] For example, the *Information Privacy Act 2000* (Vic) has an objects clause covering such matters as balancing the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector.[42] The Act then requires the Privacy Commissioner to have regard to the objects of the Act in the performance of his or her functions and the exercise of his or her powers under the Act.[43]

Submissions and consultations

43.26 The ALRC asked in IP 31 whether these constraints on the exercise by the Privacy Commissioner of his or her powers are appropriate.[44] Most submissions received by the ALRC argued that the constraints were appropriate and supported the retention of s 29 of the *Privacy Act*. For example, the OPC expressed support for the premise that privacy is a right that must be balanced with other community interests and supported the continued inclusion of s 29 as a clear statement acknowledging this context.[45] Similarly, the Queensland Council for Civil Liberties saw no reason to alter the constraints imposed by the Act on the exercise of the powers by the Commissioner,[46] and the Investment and Financial Services Association submitted 'that the present powers of the Commissioner are adequate and provide a reasonable

38 Explanatory Memorandum, Privacy Bill 1988 (Cth), 37.
39 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 28.
40 *Privacy Act 1993* (NZ) s 14. See also *Information Privacy Act 2000* (Vic) s 60.
41 This is the approach taken in a number of jurisdictions, including: *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 3; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recitals 2, 3; art 1. See also the Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).
42 *Information Privacy Act 2000* (Vic) s 5.
43 Ibid s 60.
44 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–2.
45 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
46 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

balance between protecting people's privacy yet not imposing undue additional costs and compliance on industry'.[47]

43.27 In contrast, the APF submitted that successive Commissioners appear to have interpreted s 29(a) as limiting their ability to perform the role of public advocate and champion of privacy, which the AFP describes as an unfortunate and unnecessary interpretation.[48]

ALRC's view

43.28 The ALRC proposes in Chapter 3 that the *Privacy Act* be amended to include an objects clause.[49] In that proposal, the ALRC suggests objects that draw on similar themes to those in s 29, including to implement Australia's obligations at international law in relation to privacy and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests. The ALRC is of the view that s 29 should be amended to require the Commissioner to have regard to the proposed objects of the Act in performing his or her functions and exercising his or her powers. This is consistent with a purposive approach to statutory interpretation, which requires that in interpreting a provision of an Act, a construction that promotes the purpose or object underlying the Act should be preferred to a construction that would not promote that purpose or object.[50]

43.29 Aligning the matters to which the Privacy Commissioner must have regard with the objects of the *Privacy Act* also ensures that everyone interpreting, applying and attempting to understand the Act—whether they are agencies, organisations, lawyers, academics or the OPC itself—has regard to the same set of objects. By moving the factors set out in s 29 to the objects clause, the Act effectively indicates that, not only are the enumerated factors critical in influencing the Privacy Commissioner's administration of the Act, they are also critical in directing the general public's understanding and interpretation of the Act.

Proposal 43–3 Section 29 of the *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act, as set out in Proposal 3–4, in the performance of his or her functions and the exercise of his or her powers.

---

47 Investment and Financial Services Association, *Submission PR 122,* 15 January 2007.
48 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
49 Proposal 3–4.
50 *Acts Interpretation Act 1901* (Cth) s 15AA.

Accountability mechanisms

43.30 The Privacy Commissioner and the OPC are subject to a number of accountability mechanisms to ensure that decisions made, and conduct engaged in, by the Commissioner and OPC are legal and correct. These mechanisms include judicial review, merits review and review by the Commonwealth Ombudsman.

43.31 In addition to the review rights that, as discussed below, are primarily held by individuals (in the sense that an individual can initiate them through making a complaint or instituting proceeding), the Commissioner is also subject to another form of accountability—that is, the Commissioner is subject to parliamentary scrutiny with regard to the substance of legislative instruments issued by the Commissioner. Most of the binding instruments issued by the Commissioner—such the s 17 Tax File Number Guidelines and public interest determinations[51]—are 'disallowable instruments', which means they are subject to parliamentary oversight and disallowance under the *Legislative Instruments Act 2003* (Cth). This provides further oversight and scrutiny of the substance of decisions made by the Commissioner.

Judicial review

43.32 Complainants and respondents may apply under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (the ADJR Act) to the Federal Court or Federal Magistrates Court for a review of 'administrative decisions', or 'conduct' preparatory to the making of a decision by the Privacy Commissioner under the *Privacy Act*.[52]

43.33 The ADJR Act provides an aggrieved person with broad grounds to apply for review. These grounds include a breach of natural justice; error of law; and an improper exercise of power, which includes having an improper purpose, taking an irrelevant consideration into account, failing to take a relevant consideration into account, an abuse of power, and unreasonableness.[53]

43.34 Judicial review is to be distinguished from merits review. Under the ADJR Act, the court reviews the legality of the process followed to make the decision, not the substance of the decision (which is the subject of merits review). The court cannot hear the matter afresh or substitute the decision of the Commissioner with its own. If the court finds that the grounds for review are made out, it can make an order setting aside

---

51 Other disallowable instruments issued by the OPC include the *Credit Reporting Code of Conduct*, and determinations made under Part IIIA. Note that privacy codes approved under Part IIIAA of the *Privacy Act* are legislative instruments but are not subject to disallowance by Parliament: see *Legislative Instruments Act 2003* (Cth) s 44(2), Item 44; *Legislative Instruments Regulations 2004* (Cth) sch 2, Item 8.

52 *Administrative Decisions (Judicial Review) Act 1977* (Cth) ss 3, 5, 6.

53 Ibid ss 5, 6.

or quashing the decision and can remit the matter back to the Privacy Commissioner for further reconsideration according to law.[54]

43.35 Matters that could be the subject of an application for review under the ADJR Act include a decision not to investigate (or investigate further) a privacy complaint under s 41, a decision not to make a determination under s 52, and a failure to give reasons to a person adversely affected by a decision of the Commissioner.[55]

Merits review

43.36 As noted above, merits review is concerned with the substance of a decision and, in particular, whether the decision was the correct or preferable decision. There are very limited rights to merits review under the *Privacy Act*. There is a right to apply to the Administrative Appeals Tribunal for a review of the Commissioner's decision to refuse to approve the medical research and genetics guidelines under ss 95, 95A and 95AA of the *Privacy Act*.[56]

43.37 Secondly, merits review is available in respect of determinations against agencies, but only in relation to decisions made to include or not include a declaration for compensation or costs.[57] Merits review is not available for other decisions made by the Privacy Commissioner in the complaints process. For instance, there is no right to merits review of a decision by the Commissioner under s 41 of the Act not to investigate a complaint, or to cease investigations, on the basis that the Commissioner considers that the respondent has adequately dealt with the complaint, regardless of whether the complainant is satisfied with the respondent's response.[58]

Commonwealth Ombudsman

43.38 The Commissioner and the OPC are also subject to review by the Commonwealth Ombudsman with respect to 'a matter of administration'.[59] The Ombudsman is an independent statutory office holder who can investigate administrative actions of Australian Government officials and agencies, such as the OPC, either on receipt of a complaint or on the Ombudsman's own motion. The Ombudsman investigates and resolves disputes through consultation and negotiation, and, where necessary, by making formal, non-binding recommendations to senior

---

54 Ibid s 16. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 129.

55 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 129; *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 16.

56 See *Privacy Act 1988* (Cth) ss 95(5), 95A(7), 95AA(3). Under s 95A(7), an application may also be made to the Administrative Appeals Tribunal for review of a decision of the Commissioner to revoke an approval of guidelines.

57 Ibid s 61. Merits review is discussed in detail in Ch 45.

58 See the concerns raised about this point in Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 138–139.

59 *Ombudsman Act 1976* (Cth) s 5; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

levels of government. The type of actions the Ombudsman may report on include where the action: appears to have been contrary to law; was unreasonable, unjust, oppressive or improperly discriminatory; or was otherwise, in all the circumstances, wrong.[60]

43.39 The Ombudsman and the OPC entered into a memorandum of understanding (MOU) in November 2006. The MOU addresses a number of issues and is intended to ensure, amongst other things, that complaints made to one party about the other are handled efficiently and fairly.

Submissions and consultations

43.40 As noted above, the ALRC asked in IP 31 whether the constraints imposed in the *Privacy Act* on the exercise by the Commissioner of powers conferred by the Act are appropriate.[61] The Consumer Credit Legal Centre (NSW) commented on the liability of the OPC to judicial review, submitting that despite the possibility of judicial review in some circumstances, 'there is no real oversight in relation to the quality of decision-making as there is a lack of any form of merits review'.[62] A number of other stakeholders also commented on the issue of merits review of complaint determinations, and the issue is discussed in detail in Chapter 45.

ALRC's view

43.41 The ALRC considers that the current accountability mechanisms of judicial review and review by the Commonwealth Ombudsman are appropriate. The fact that the Commissioner's decisions are subject to judicial review is an important oversight mechanism to ensure the legality of the exercise of the Commissioner's powers and that proper processes are followed. The oversight by the Ombudsman is consistent with other federal regulators, and provides a necessary avenue for individuals who have a complaint against the administrative workings of the OPC.

43.42 The ALRC does not, however, think the current rights to merits review are sufficient, particularly in relation to complaint determinations. The concerns raised by stakeholders about the inability to challenge the merits of the Commissioner's decisions are addressed in Chapter 45, with a proposal made to provide merits review of determinations made by the Commissioner under s 52 of the *Privacy Act*.[63]

---

60 *Ombudsman Act 1976* (Cth) s 15(1). There are a number of other circumstances set out in this section.

61 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–2.

62 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

63 Proposal 45–7.

Criminal liability

Background

43.43 The Commissioner and his or her staff and delegates are subject to criminal liability in some circumstances. It is an offence for the Commissioner or a member of his or her staff (present and past) to disclose, use or make a record of information acquired about a person in the performance of that role, other than to do something permitted or required by the *Privacy Act*.[64] Such a person is not obliged to divulge or communicate that information except as required or permitted by the *Privacy Act*.[65] Similar secrecy provisions are found in other federal legislation and state privacy legislation.[66]

Submissions and consultations

43.44 The OPC supported the retention of the above provisions, submitting that they were consistent with secrecy and non-disclosure provisions in other Commonwealth legislation.[67]

ALRC's view

43.45 The ALRC considers the current secrecy provisions are appropriate and has not made any proposals on these matters. The liability of the Commissioner to criminal sanctions for disclosure of certain information is appropriate and the provisions, as noted above, are consistent with other relevant legislation.

Immunity

Background

43.46 The Commissioner, and any person acting under his or her direction or authority, has immunity from civil action for acts done in good faith in the exercise of any power conferred by the *Privacy Act*.[68] This immunity also extends to an adjudicator under an approved privacy code and his or her delegate.[69] Privacy legislation in state, territory and overseas jurisdictions provides similar immunities to

---

64 *Privacy Act 1988* (Cth) s 96(1), (3). The offence is punishable by a penalty of $5,000 or imprisonment for 1 year, or both. Note that the OPC released its new layered privacy policy (which sets out its personal information handling practices) in August 2006: Office of the Privacy Commissioner, *Privacy Policy* (2006).

65 *Privacy Act 1988* (Cth) s 96(2), (4).

66 See, eg, *Ombudsman Act 1976* (Cth) ss 35, 35A; *Migration Act 1958* (Cth) s 377; *Privacy and Personal Information Protection Act 1998* (NSW) s 67; *Information Privacy Act 2000* (Vic) s 67.

67 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

68 *Privacy Act 1988* (Cth) s 64(1).

69 Ibid s 64.

privacy commissioners,[70] and precedent for immunity can also be found in the *Ombudsman Act 1976* (Cth).[71]

43.47 The *Privacy Act* also provides that civil action will not lie against a person in respect of loss, damage or injury suffered by another person because of certain acts done in good faith. These acts are: the making of a complaint under the Act or under an approved code; the acceptance of a complaint under s 40(1B); or the making of a statement to, or giving a document of information to, the Privacy Commissioner.[72] Similar immunity for complainants can be found in privacy legislation in Australian states and territories.[73]

43.48 In addition, persons who give information, produce a document or answer a question when directed to do so by the Commissioner are not liable to penalties under other Acts.[74]

Submissions and consultations

43.49 The ALRC asked in IP 31 whether the scope of immunities conferred on the Privacy Commissioner, adjudicators and other persons are appropriate.[75] The OPC supported the continuation of the immunity from civil actions provided to the Commissioner (or code adjudicator) and their delegates. The OPC also supported the protection from civil action provided to complainants, explaining that 'this is fundamental to providing individuals with an opportunity to freely raise a complaint without concern that they may be liable for defamation or other civil action'.[76]

43.50 The APF also described these immunities as important and suggested that 'the law should confirm that the protection extends to bodies bringing representative complaints and otherwise drawing privacy compliance issues to the attention of the Commissioner and the public'.[77]

---

70 For examples in other Australian privacy legislation, see, *Privacy and Personal Information Protection Act 1998* (NSW) s 66; *Information Act 2002* (NT) s 151. For examples in overseas jurisdictions, see *Privacy Act* RS 1985, c P-21 (Canada) s 67; *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) s 22; *Crown Entities Act 2004* (NZ) s 121.

71 *Ombudsman Act 1976* (Cth) s 33.

72 *Privacy Act 1988* (Cth) s 67.

73 *Privacy and Personal Information Protection Act 1998* (NSW) s 66A; *Information Privacy Act 2000* (Vic) s 66; *Information Act 2002* (NT) s 152.

74 *Privacy Act 1988* (Cth) s 44(5).

75 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–4.

76 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

77 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

ALRC's view

43.51 The ALRC considers the current immunity afforded to the Privacy Commissioner and code adjudicators, and their delegates, is appropriate. The ALRC does not, at this stage, make any proposals in this area.

43.52 The ALRC also does not propose any changes to the current formulation in s 67 of the *Privacy Act*, which provides protection from civil action to a person who, in good faith, makes a complaint under this Act. A complaint can only be made under s 36 of the Act, whether it be an IPP complaint, an NPP complaint, or a representative complaint.[78] The ALRC is of the view that a person or body who lodges a representative complaint under s 36 would enjoy protection from civil action where the act was done in good faith, because the protection in s 67 does not distinguish between the type of complaint made or the person who made the complaint; it applies to the act of making the complaint.

43.53 The ALRC notes, however, that there does not appear to be any guidance on the OPC website as to the protection offered to complainants who make complaints in good faith. It would be useful for the OPC to make this protection clear in the document setting out its complaint-handling policies and procedures, as anticipated in Proposal 45–8. This is particularly important given that, as recognised by the OPC, the protection is fundamental to ensuring that complainants feel safe in raising complaints. In issuing such guidance, it would be helpful to indicate clearly that s 67 applies to individuals and bodies bringing representative complaints in the same way that it applies to individual complainants.

43.54 The ALRC does not believe that the *Privacy Act* should be amended to confirm that the protection from civil action extends to bodies that otherwise draw privacy compliance issues to the attention of the Commissioner and the public.[79] In relation to issues brought to the attention of the Commissioner, s 67(b) already makes it clear that the protection from civil action extends to making a statement or giving a document or information to the Commissioner, whether or not required by s 44 of the *Privacy Act*.[80] This too, however, could be clarified further in the proposed complaint-handling policy and procedures document.

43.55 In relation to the suggestion that issues brought to the attention of the public should also attract immunity, the ALRC does not believe that such a protection can be justified. The ALRC is not aware of examples of such protection being offered for disclosures to the public in any other privacy legislation. The ALRC is of the view that

---

78 See the respective definitions of each in *Privacy Act 1988* (Cth) s 6(1).

79 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

80 Note also that the Explanatory Memorandum to the Privacy Bill 1988 explained that s 67 'precludes a person from being sued for lodging a complaint with the Commissioner or providing him/her with information where those acts are done in good faith': Explanatory Memorandum, Privacy Bill 1988 (Cth), 59.

the OPC is the appropriate body with which to raise compliance issues. If a body wants to disclose the issues to the public, then it should bear any subsequent risks.

Privacy Advisory Committee

Composition

43.56 The *Privacy Act* establishes a Privacy Advisory Committee (Advisory Committee) consisting of the Commissioner and not more than six other members, of which the Commissioner is convenor.[81] The Governor-General appoints members (other than Privacy Commissioner) as part-time members who hold office for up to 5 years. Members are not remunerated for their service, but enjoy similar protections as the Commissioner against removal,[82] and have an obligation to disclose any conflicts of interest.[83]

43.57 The *Privacy Act* provides membership criteria for the Advisory Committee in two ways. First, it specifies that officers, employees and staff of the Commonwealth must never be in the majority on the Advisory Committee.[84] Secondly, it provides a list of membership criteria.[85] The Advisory Committee is currently constituted by the Commissioner and six members.[86] The membership criteria, and the current appointees under each criterion, are set out in the following table.

Table 43.1 Current Members of the Privacy Advisory Committee

Privacy Act	Description	Current Member
s 82(7)(a)	at least five years' high-level experience in industry, commerce, public administration or government service	Suzanne Pigdon, Former Privacy and Customer Advocacy Manager, Coles Myer Group Joan Sheedy, Assistant Secretary, Information Law Branch, Attorney-General's Department
s 82(7)(b)	at least five years' experience in the trade union movement	Associate Professor John M O'Brien, School of Organisation and Management, University of New South Wales

81 *Privacy Act 1988* (Cth) s 82(1)–(5). See also s 87 regarding meetings of the Advisory Committee.
82 Ibid s 85.
83 Ibid s 86.
84 Ibid s 82(6).
85 Ibid s 82(7).
86 See Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 31 July 2007.

s 82(7)(c)	extensive experience in electronic data-processing	Peter Coroneos, Chief Executive Officer, Internet Industry Association
s 82(7)(d)	representing general community interests, including social welfare	Dr William Pring, Director of Consultation-Liaison, Psychiatry Services Box Hill Hospital
s 82(7)(e)	extensive experience in the promotion of civil liberties	Robin Banks, Chief Executive Officer, Public Interest Advocacy Centre Ltd and Director, Public Interest Law Clearing House Inc

43.58 Membership of the Committee was developed 'to represent a variety of community interest groups'.[87] No changes or additions were made to the membership criteria of the Advisory Committee following the introduction of the credit reporting provisions in 1990 or following the inclusion of the private sector provisions in 2000.

Functions

43.59 The *Privacy Act* specifies that the Advisory Committee has functions to advise the Commissioner (whether or not requested) on matters relevant to the Commissioner's functions, recommend material for inclusion in guidelines to be issued by the Commissioner, and engage in and promote community education and consultation for the protection of individual privacy, subject to any directions given by the Commissioner.[88]

43.60 The OPC sets out on its website the terms of reference for the Advisory Committee, which are based on the functions set out in the *Privacy Act*. The OPC notes that the terms of reference 'assume a strategic advisory role' for the Advisory Committee and include:

- advising the Privacy Commissioner on privacy issues, and the protection of personal information;
- providing strategic input to key projects undertaken by the Privacy Commissioner;
- fostering collaborative partnerships between key stakeholders to promote further the protection of individual privacy;

87 Explanatory Memorandum, Privacy Bill 1988 (Cth), 4. Previous members of the Advisory Committee have been drawn from the Australian Consumers' Association, the Australian Chamber of Commerce and Industry, the Australian Information Industry Association and the Human Rights and Equal Opportunity Commission.

88 *Privacy Act 1988* (Cth) s 83.

- promoting the value of privacy to the Australian community, business and government; and

- supporting office accountability to external stakeholders.[89]

43.61 In its most recent annual report, the OPC described the Advisory Committee as acting 'as an external reference point that supports the Commissioner in gaining access to the broad views about privacy in the private sector, government and the community at large'.[90] In the past, the Advisory Committee has assisted the OPC by providing strategic advice about such matters as the review of the private sector provisions of the *Privacy Act* in 2004–05,[91] and the 25th International Conference of Data Protection and Privacy Commissioners in 2003–04.[92] The Advisory Committee has also provided input into guidelines developed by the OPC, as well as advice about the OPC's complaints processes and the publication of complaint case notes.[93]

43.62 The Privacy Commissioner can convene such meetings of the Advisory Committee as he or she considers necessary for the performance of the Committee's functions.[94]

Submissions and consultations

43.63 The ALRC asked in IP 31 whether the Advisory Committee performs a useful role with appropriate powers and functions; whether the fields of expertise represented on the Advisory Committee are appropriate; and whether the Advisory Committee, including the fields of expertise, need to be set out in the *Privacy Act*.[95] The ALRC received a number of submissions in response to the first two parts of this question.

43.64 In relation to the general functions and powers of the Advisory Committee, the OPC submitted that it supported the continuation of the Advisory Committee in its current role as an independent advisory body. The OPC considered that the

---

89 Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 31 July 2007.

90 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 23.

91 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 29.

92 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 47.

93 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 29; Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 47; Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 23.

94 *Privacy Act 1988* (Cth) s 87.

95 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–3.

Committee's powers and functions are appropriate and found that the Committee provides valuable input into policy development and general strategic discussion.[96]

43.65 In contrast, the APF submitted that:

> The Privacy Advisory Committee may perform a useful function 'behind the scenes', but it is almost invisible to the public. Members do not seem to have seen themselves as accountable to the constituencies which might be inferred from the criteria for appointment and have rarely sought to consult with constituencies.
>
> The objectives of the Advisory Committee might be better performed by separate committees representing business, government and consumer interests respectively, with independent secretariats and public reporting requirements.[97]

43.66 In terms of additional functions, the National Association for Information Destruction submitted that the Advisory Committee could have a role in establishing a standard for secure document destruction.[98]

43.67 Stakeholders also commented on the membership criteria of the Advisory Committee. The OPC submitted that the membership criteria should be reviewed and updated to reflect current business, community and government environments. In particular, the OPC expressed strong support for the introduction of an explicit requirement that a health sector representative be included on the Advisory Committee given the community concern regarding health privacy.[99] Another submission went further and suggested there be two designated positions for the health sector: a consumer (from an advocacy organisation) and a practitioner.[100]

43.68 The OPC also suggested that the criteria in s 82(7)(a) be amended to require separately the inclusion of a member with high level experience in industry or commerce *and* a member with experience in public administration or government, rather than combining these categories.[101] The OPC did not give a reason for this recommendation.

43.69 Other suggestions by stakeholders for membership to the Advisory Committee included:

---

96 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

97 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

98 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

99 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

100 Confidential, *Submission PR 134,* 19 January 2007. The APF's submission to the Senate Legal and Constitutional Reference Committee inquiry into the *Privacy Act* also recommended that a separate position be 'reserved' for a representative of health issues, given the importance of the issue: Australian Privacy Foundation, *Supplementary Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988 concerning the Privacy Advisory Committee*, 1 March 2005, 3.

101 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

- an information technology security professional;[102]
- a representative from the Institute of Mercantile Agents;[103]
- a representative from the Council of Small Business Organisations of Australia;[104] and
- a privacy advocate.[105]

43.70 The OPC also suggested that the terminology used in the membership criteria—such as requiring a person with extensive experience in 'electronic data-processing'—should be updated to better reflect current data-handling practices.[106] Electronic data-processing is not a term used throughout the *Privacy Act*.[107]

43.71 Two alternative terms that could replace electronic data-processing are 'information technology' or 'information and communication technologies'. The phrase 'technologies' in this context is likely to be too broad and may lose meaning. The term 'information technology' is generally understood to mean 'the use of computers to produce, store and retrieve information'[108] and encapsulates the notion of 'electronic data-processing'.[109] 'Information and communication technologies' is a modern development on 'information technology' and is intended to broaden the term explicitly to include all types of electronic communications. The term has been used to describe how information is 'produced, collected, sorted, filtered, transmitted, communicated, interpreted and stored'[110] and is used by a number of organisations throughout the world, including the European Commission, World Bank, and Organisation for Economic Co-operation and Development.

---

102 W Caelli, *Submission PR 99,* 15 January 2007.
103 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
104 Ibid.
105 Confidential, *Submission PR 134,* 19 January 2007.
106 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
107 'Electronic data-processing' is in fact only used in s 82(7)(c) of the *Privacy Act 1988* (Cth). 'Data processing' is used once in the *Privacy Act*, in s 27(1)(c). The use of 'processing' has its heritage in the Council of Europe Convention: see *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force generally on 1 October 1985).
108 *Macquarie Dictionary* (online ed, 2005).
109 The ALRC notes that the OPC website already refers to 'information technology' in describing the range of perspectives on the Advisory Committee: see Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 31 July 2007.
110 Commonwealth Scientific and Industrial Research Organisation, *Information and Communication Technology Overview* (2007) <www.csiro.au/org/ICTOverview.html> at 31 July 2007.

Options for reform

43.72 There are two main options for reform in this area. The first is to retain the current structure of the Committee, but make any necessary amendments to the membership requirements to reflect contemporary issues and community concerns. The second option is to change the Committee's legislative structure to make it a more flexible, informal body with a more projects or inquiry-oriented role. This could involve changing the appointment process, so that members are not statutory appointees for a set term, but are appointed by the Privacy Commissioner. Instead of mandating membership criteria, the Act could require that the Committee is broadly representative of the general community and give suggestions as to criteria to achieve broad representation. This kind of membership structure would give the OPC flexibility to set up an Advisory Committee with specific expertise to assist with a particular project.

43.73 Examples of this more flexible model are found in the *Human Rights and Equal Opportunity Act 1986* (Cth). Under this Act, the Minister is required to establish at least one advisory committee to perform such functions as the Minister directs, including advising HREOC in relation to the performance of the Commissioner's functions, and reporting to the Minister on certain matters.[111] HREOC itself may also establish advisory committees to advise the Commission, with the approval of the Minister.[112]

ALRC's view

43.74 The Privacy Advisory Committee should continue in its current form, but with some amendments to the membership criteria. As statutory appointees, the members enjoy independence and protection from removal, allowing them to express views without fear or favour. Leaving the members as statutory appointments by the Governor-General insulates the Commissioner from allegations of bias in relation to a particular appointment. The Commissioner, however, may still make recommendations to the appropriate minister for appointments.

43.75 In order to give the Commissioner additional flexibility, however, the ALRC proposes that the Commissioner be given an express power to establish expert panels to assist with specific projects. This is discussed further below.

43.76 In terms of changes to the existing structure of the Privacy Advisory Committee, the ALRC is of the view that, given the significance of privacy in the health sphere and the impact of health privacy on every member of the community, it is appropriate that a health perspective is represented on the Advisory Committee.[113]

---

111 *Human Rights and Equal Opportunity Act 1986* (Cth) s 17(1).

112 Ibid s 17(2).

113 The ALRC notes that under the current criteria, a health representative could be appointed within the ambit of s 82(7)(d). However, it is the ALRC's view that it would be more beneficial to fill this criterion

43.77 At this stage, the ALRC does not believe that it is necessary that the membership criteria in s 82(7)(a) be separated. While the ALRC sees a benefit in having a government *and* industry representative on the Committee, representatives from both government and business can be appointed under the current membership structure. The Act only specifies five categories of members but allows the appointment of six members. Specifying six categories of membership (that is, including the new health category) and allowing for the appointment of seven members in addition to the Commissioner could be used to achieve the same result.

43.78 There are, however, two alternative approaches on this issue that could be adopted. The first is to separate the membership criteria and allow for one appointment per category (that is, specify seven categories and allow for seven members). The second is to separate the membership criteria, which would create seven categories of membership, and allow for the appointment of one member per category plus one member at large—equalling eight members together.

43.79 If the membership category in s 82(7)(a) was separated, the ALRC is of the view that the second option is preferable to the first, as it retains the flexibility to appoint persons beyond the confines of the membership criteria in the Act and allows for the appointment of more than one person to a membership category. The ALRC is concerned, however, that the second option increases the size of the Committee, which may affect the functioning and flexibility of the body itself, and may shift the preponderance of views on the Committee to the regulated entities—that is, to the government, business, health and data-processing sectors. While the Act specifies that a majority of appointed persons cannot be officers or employees of the Commonwealth, there is no such limitation against business or industry views.

43.80 Given the proposed objects of the Act, it is important that the Advisory Committee provide the Commissioner with a balanced range of views from both the regulated entities and from consumer and privacy advocates. Given these concerns, the ALRC's preliminary view is to retain the current compound category in s 82(7)(a).

43.81 In relation to the other membership criteria put forward by stakeholders, the ALRC is of the view that each suggestion could already be addressed under the existing membership criteria. It is important to keep the criteria at a high level, to enable a variety of backgrounds and stakeholders to be represented. If specific expertise is required for a particular project, expert panels could be utilised.

---

with a representative from the social and community welfare sector more generally, and to require, in addition to that member, a further member representing the health sector.

43.82 With regard to terminology, the ALRC's view is that the reference to 'electronic data-processing' in the membership criterion should be replaced with 'information and communication technologies', to reflect more contemporary practices and parlance. The ALRC prefers 'information and communication technologies' to 'information technology', as it is broader and more clearly encapsulates the notion of electronic communications.

Expert Panels

43.83 In order to give the Commissioner flexibility to solicit expertise in undertaking projects or inquiries, the ALRC is of the view that the Commissioner should have the power to convene temporary or standing expert panels. While it is not technically necessary to include such a power in the Act—as the Commissioner could convene such committees already without an express power—it would be consistent with the approach taken with the Privacy Advisory Committee, which is prescribed in the *Privacy Act*. It is also consistent with the approach taken in the *Human Rights and Equal Opportunity Act*.[114]

43.84 The use of expert panels could address some of the suggestions raised by stakeholders about appointing more specific expertise to the Advisory Committee. For example, as noted above, the National Association for Information Destruction submitted that the Advisory Committee could have a role in establishing a standard for secure document destruction, in which case the Association suggests the Committee should include representatives from the secure information destruction industry.[115] In this instance, rather than mandating a permanent representative on the Advisory Committee, a better route would be to create an expert panel with representatives from the document destruction industry to provide expertise to the OPC in developing the standard.[116]

43.85 Expert panels could also be used to assist the OPC in the development of education and guidance materials in relation to new and developing technologies. This is discussed further in Part B of the Discussion Paper.

Proposal 43–4 Section 82 of the *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee:

(a) require the appointment of a person to represent the health sector;

(b) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven; and

114 *Human Rights and Equal Opportunity Act 1986* (Cth) s 17.
115 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.
116 See Ibid.

(c) replace 'electronic data-processing' in s 82(7)(c) with 'information and communication technologies'.

Proposal 43–5 The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion to advise the Privacy Commissioner.

44. Powers of the Office of the Privacy Commissioner

Contents

Introduction 1186
Oversight powers 1186
- Advice functions 1186
- Research and monitoring functions 1187
- Education functions 1188
- Submissions and consultations 1189
- ALRC's view 1191
- Summary of proposals made in relation to education 1192

Guidelines 1193
- Power to issue non-binding guidelines 1193
- Power to issue binding guidelines 1194
- ALRC's view 1195

Personal Information Digest 1196
- Background 1196
- Submissions and consultations 1197
- ALRC's view 1198

Privacy impact assessments 1199
- Background 1199
- PIAs in other jurisdictions 1202
- Submissions and consultations 1203
- Options for reform 1207
- ALRC's view 1208

Compliance powers 1210
Audit functions 1211
- Background 1211
- Audits of organisations 1212
- Submissions and consultations 1214
- ALRC's view 1216

Self-auditing 1218
- Background 1218
- Submissions and consultations 1219
- ALRC's view 1220

Functions under other Acts 1221
- Background 1221
- Submissions and consultations 1222
- ALRC's view 1222

Public interest determinations 1223
Background 1223
Nature of determinations 1223
Temporary public interest determinations 1224
Submissions and consultations 1224
ALRC's view 1225
Privacy codes 1226
Background 1226
Binding Codes 1228
Submissions and consultations 1231
ALRC's view 1234

Introduction

44.1 This chapter examines the functions vested in the Privacy Commissioner (Commissioner). These functions include powers to oversee the *Privacy Act 1988* (Cth) and to monitor compliance with the Act.[1] The chapter also discusses privacy impact assessments and the Commissioner's functions in issuing public interest determinations and administering the code provisions in the Act.

Oversight powers

44.2 The Commissioner's functions in overseeing the operation of the *Privacy Act* include: giving advice; providing research and monitoring of technological developments; and conducting education. The Commissioner also has oversight functions in relation to tax file numbers and credit reporting.[2]

Advice functions

44.3 The Commissioner has several advisory functions under the *Privacy Act*. These are to:

- Provide advice to a minister, agency or organisation on any matter relevant to the operation of the *Privacy Act*.[3] A related function is to inform the Minister of

1 The Commissioner's complaint handling and enforcement powers are discussed in Chs 45 and 46.

2 The general approach of the *Privacy Act* is to state the Commissioner's 'functions' and give the Commissioner 'power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions': *Privacy Act 1988* (Cth) ss 27(2), 28(2), 28A(2).

3 Ibid s 27(1)(f). See also the equivalent function in credit reporting: s 28A(1)(f).

action that needs to be taken by an agency to comply with the Information Privacy Principles (IPPs).[4]

- Examine any proposal for data-matching or data linkage that may involve an interference with the privacy of individuals or may otherwise affect adversely the privacy of individuals, and to ensure that any adverse effects are minimised.[5]

- Examine any proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be an interference with the privacy of individuals or which may otherwise affect adversely the privacy of individuals and to ensure that any adverse effects are minimised.[6]

- Make reports and recommendations to the Minister in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of individuals' privacy.[7]

- Provide advice to tax file number (TFN) recipients about their obligations under the *Taxation Administration Act 1953* (Cth) and on any matter relevant to the operation of the *Privacy Act*.[8]

- Provide advice to the adjudicator appointed under a privacy code on any matter relevant to the operation of the *Privacy Act* or the relevant privacy code.[9]

44.4 In 2005–06, the Commissioner used her advice functions to prepare 155 advices on significant policy issues. As described in the Annual Report of the Office of the Privacy Commissioner (OPC), the advices included: letters and emails to government departments, agencies and organisations on specific proposals; submissions to public consultation processes and Senate inquiries; advices for guidance material published by the Commissioner; and advices for inclusion in other reports and published documents.[10]

Research and monitoring functions

44.5 Another aspect of the Commissioner's functions in overseeing the *Privacy Act* is undertaking research into, and monitoring developments in, data processing and

---

4 Ibid s 27(1)(j). Currently, the relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

5 *Privacy Act 1988* (Cth) s 27(1)(k).

6 Ibid s 27(1)(b). This power, and the related concept of privacy impact assessments, is discussed separately below.

7 Ibid s 27(1)(r). Currently, the relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

8 *Privacy Act 1988* (Cth) s 28(1)(g).

9 Ibid s 27(1)(fa).

10 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 4.

computer technology (including data-matching and data linkage) to minimise their adverse effects on the privacy of individuals and to report to the Minister about the results of such research and monitoring.[11] The Commissioner also has the function of monitoring and reporting on the adequacy of equipment and user safeguards.[12]

Education functions

44.6 The Commissioner's oversight functions in relation to education include:

- promoting an understanding and acceptance of the IPPs and National Privacy Principles (NPPs) and of the objects of those principles;[13] and

- undertaking educational programs on the Commissioner's own behalf or in cooperation with other persons or authorities acting on behalf of the Commissioner, for the purpose of promoting the protection of individual privacy.[14]

44.7 The OPC has said that a factor likely to increase 'community confidence that individuals' rights are protected' is 'raising awareness about individuals' privacy rights'.[15] To this end, the OPC provides information through its information hotline and its website (which contains various OPC publications). Awareness of the existence of the OPC's website has increased each year.[16]

44.8 Considerable attention was given to the Commissioner's education power in the OPC review of the private sector provisions of the *Privacy Act* (OPC Review) and the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry). Overall, the submissions acknowledged that education by the OPC plays a vital part in promoting community awareness of privacy laws. It was suggested in several submissions that public awareness be raised, using either one-off or regular campaigns. It was also suggested that sectors of the community with low awareness of privacy rights be targeted, and that campaigns address not only individuals' rights, but also the rights and obligations of organisations.[17]

---

11 *Privacy Act 1988* (Cth) s 27(1)(c). Currently, the relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

12 *Privacy Act 1988* (Cth) s 27(1)(q). The use of these powers in relation to new and developing technologies is discussed further in Part B.

13 Ibid s 27(1)(d).

14 Ibid s 27(1)(m).

15 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 105.

16 See Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 19–20.

17 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 107–111. See also Parliament of Australia—Senate Legal and

44.9 Both reviews called for the OPC to be funded adequately. It was said that this would facilitate a shift in focus from complaint handling to education. In the OPC Review, the OPC noted that '[s]ince the implementation of the private sector provisions, the Office has shifted resources from its guidance and advice role to its compliance role to try to better manage and resolve the complaints received'.[18] It recognised, however, that 'organisations need more guidance'[19] and recommended that the Government consider specifically funding the Office to undertake a systematic and comprehensive education program to raise community awareness of privacy rights and obligations.[20]

44.10 Following the OPC Review, the Government made a commitment to provide additional funding to the OPC over the next four years. In response, the OPC has stated that this could

> allow us to respond to calls from business and industry for greater assistance in meeting their obligations under the *Privacy Act*. Following on from recommendations made in my 2005 review of the private sector provisions of the *Privacy Act*, my Office will work closely with business and consumer representatives to develop guidance and educational material to assist organisations and individuals to better understand their rights and responsibilities under the *Privacy Act*.[21]

Submissions and consultations

44.11 The ALRC asked in the Issues Paper, *Review of Privacy* (IP 31) whether the Commissioner's powers to oversee the *Privacy Act* were appropriate and effectively exercised.[22] The OPC submitted generally that the Commissioner's oversight powers are appropriate and should be retained.[23]

44.12 The Office of the Information Commissioner Northern Territory submitted that the OPC's advice on policy and legislative developments must remain a key feature of its operations.[24] Other stakeholders requested more timely advice and assistance from the OPC. The Consumer Credit Legal Centre (NSW) (CCLC) submitted that while the Commissioner's legislative power to provide advice is appropriate, 'its exercise is not always effective nor does it always produce fair outcomes for consumers'.[25] In

---

Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 145.

18 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 5.

19 Ibid, 7.

20 Ibid, recs 26, 48. The Senate Committee privacy inquiry made a similar recommendation: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 19.

21 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 2–3.

22 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–5.

23 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

24 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

25 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. Similar comments were made in Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

particular, the CCLC submitted that any advice given by the Commissioner in relation to any matter relevant to the operation of the Act should be made public, 'in order to ensure the transparency and fairness of OPC's operations'.

44.13 In relation to the research and monitoring function, the OPC submitted that the reference in s 27(1)(c) to 'computer technology' is outdated and 'may inadvertently restrict the operation of this clause which the Office believes is intended to provide for research into technologies with a possible privacy impact, whether or not they are computer-based'.[26] The OPC recommended that the section be amended by replacing 'computer technology' with wording that would encompass all technologies that could possibly impact on an individual's privacy.

44.14 The education function drew the most comment from stakeholders. Several stakeholders commented on the priority of the education function and the desire to see more guidance from the OPC to encourage understanding and compliance with the principles.[27] Stakeholders noted the preventative aspects of education—to reduce the potential for breaches of privacy and 'ill-informed reliance on privacy as a reason for refusing to take particular action'.[28]

44.15 In relation to public education, stakeholders commented on the 'utility of education materials in uplifting public confidence in, and awareness of, the OPC's ability to enforce privacy rights'.[29] Another stakeholder observed that lack of understanding of privacy regulation is often the source of complaints, with more education identified as a way to address this problem.[30] The public forums conducted by the ALRC in this Inquiry suggested low levels of awareness and understanding of privacy laws in the community. The ALRC received many stories of 'BOTPA' ('because of the *Privacy Act*') explanations being given as a reason for refusing a request for information or assistance from an agency or organisation.[31] While the extent to which such explanations are based on a proper understanding and application of the Act, rather than a deliberate excuse to avoid giving information, is not clear,

---

26 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

27 Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

28 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. The NHMRC suggested that there is 'considerable anecdotal evidence that the appropriate handling of health information for important health care and health and medical research purposes is jeopardised by a generally inadequate understanding of the law': National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

29 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. See also Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

30 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

31 H Ruglen, *Submission PR 39,* 27 June 2006; K Bottomley, *Submission PR 10,* 1 May 2006; T de Koke, *Submission PR 8,* 5 April 2006. See also Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

education may help to increase understanding and lessen the reliance on BOTPA explanations.[32]

44.16 Some stakeholders suggested that industry bodies, schools and other institutions should also bear some responsibility to educate their members, students or constituencies about privacy obligations.[33] It was suggested, for example, that privacy should be taught at medical schools and in intern programs to ensure that medical students are aware of their obligations before they handle personal information about their patients. It was also suggested that human research ethics committees (HRECs), and the relevant health department, should be required to educate their researchers about relevant privacy regulation.[34]

44.17 The National Health and Medical Research Council (NHMRC) commented on the formulation of the education power, noting that the stated purpose of the Commissioner's role in s 27(1)(m) is to promote the protection of individual privacy. The NHMRC submitted that

> education about the *Privacy Act* for all stakeholders should address, in a balanced manner, individual privacy rights, the public benefit to be obtained from the controlled handling of personal information in the absence of consent in appropriate circumstances, the potential tensions between these objectives in some situations and the ways in which such tensions can be resolved in the overall public interest.[35]

44.18 The OPC commented on the importance of education in dealing with technological developments, noting, for example, that 'education of individuals who use the internet will also be important if individuals are to be proactive in protecting their privacy and managing their identities online'. The OPC suggested that the importance of education in dealing with developing technologies should be recognised expressly in s 27(1)(c) or (m), or both.[36]

ALRC's view

44.19 The Commissioner's oversight functions provide important tools to: increase understanding of federal privacy law; contribute a privacy perspective to public debates; and establish dialogue on privacy issues between the OPC and agencies and organisations. These functions enable the Commissioner to be proactive in increasing awareness and understanding of privacy to prevent non-compliance. In the ALRC's view, these functions should be as broad as possible, and resourced effectively.

---

32 See Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

33 See Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

34 B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; Menzies School of Health Research, *Consultation PC 108*, Darwin, 27 February 2007. A similar recommendation in relation to genetics education was made in Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 23–4.

35 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

36 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

44.20 The ALRC proposes one amendment to the Commissioner's oversight functions. The ALRC's view is that, given the serious impact technology can have on invading privacy or enhancing privacy protection, the Commissioner's research and monitoring function should be broad enough to enable it to research and monitor all relevant technologies.[37] Some technologies may not come within an ordinary understanding of 'computer technology', yet still raise privacy issues. Biometrics is one example. The wording of s 27(1)(c) should be broadened to allow for research and monitoring of any pertinent technologies. This can be most easily achieved by removing the reference to 'computer'. This is also consistent with the ALRC's proposal that the *Privacy Act* be technologically neutral.[38]

44.21 While the ALRC is not proposing any reform of the advice function, the ALRC notes the concerns of stakeholders that advice should be timely and public. It is preferable, therefore, that advices (or a generic form of them) are made public if they are relevant to a broader audience and would increase understanding of the *Privacy Act*. It would not be reasonable, however, to require that all advice given by the Commissioner in relation to any matter relevant to the operation of the Act be made public. A minister or an agency may approach the Commissioner for advice on a confidential basis about Cabinet proposals, or an organisation may seek advice on proposals that are commercial-in-confidence or disclose an innovation or new project. Requiring such advices to be made public may discourage agencies and organisations from approaching the OPC, which would undermine the Commissioner's oversight and advisory functions.

44.22 In relation to the education functions, the ALRC notes the concerns raised by the OPC and NHMRC but is not proposing any reform at this stage. As currently worded, the functions provide broad powers for the OPC to educate agencies, organisations and individuals on the content and objects of the privacy principles, the importance of protecting individual privacy, and the rights and obligations provided in the *Privacy Act*.

Proposal 44–1 The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c) of the *Privacy Act*.

Summary of proposals made in relation to education

44.23 The ALRC makes a number of proposals in various chapters of this Discussion Paper for further education programs to be undertaken by the OPC. For ease of reference, these proposals are to:

37 The ALRC proposes that the Commissioner use this research and monitoring function to consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations: see Proposal 7–3.

38 See Proposal 7–1.

- provide information to the public concerning the proposed statutory cause of action for invasion of privacy;[39]

- educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed;[40]

- provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, before the proposed removal of the small business exemption from the *Privacy Act* comes into effect;[41]

- develop and publish educational material about privacy issues aimed at children and young people;[42] and

- develop and publish educational material, in consultation with various bodies, that addresses the rules regulating privacy in the telecommunications industry and complaint handling about privacy in telecommunications.[43]

Guidelines

44.24 In a principles-based regime, guidance is often necessary to make the rights and obligations in the Act sufficiently certain and clear.[44] Guidance can be provided through the Commissioner's oversight functions discussed above, and through the power to issue non-binding and binding guidelines under the *Privacy Act* and other legislation.

Power to issue non-binding guidelines

Section 27(1)(e) guidelines

44.25 The Commissioner has the power to prepare and publish guidelines to assist agencies and organisations to avoid acts or practices that may be interferences with, or affect adversely, the privacy of individuals.[45] Section 27(1)(e) guidelines are advisory only and are not legally binding. Guidelines are based on the OPC's understanding of how the *Privacy Act* works and indicate some factors the Commissioner may take into

---

39 See Proposal 5–4.
40 See Proposal 7–4.
41 See Proposal 35–2.
42 See Proposal 59–2.
43 See Proposal 64–5.
44 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 14.
45 *Privacy Act 1988* (Cth) s 27(1)(e). There is an analogous power to prepare guidelines for the avoidance of acts or practices of a credit reporting agency or credit provider that may or might be interferences with the privacy of individuals: see *Privacy Act 1988* (Cth) s 28A(1)(e).

account when handling a complaint. Nothing in the guidelines limits how the OPC can handle complaints.[46] For example, the Data Matching Guidelines explain:

> While the Privacy Commissioner may take these guidelines into consideration in assessing compliance with the [IPPs], these guidelines aim to encourage a higher standard of regard for people's privacy rights in relation to data-matching than is required by bare compliance with the IPPs and an agency would not necessarily breach the IPPs if it did not adhere to these guidelines.[47]

44.26 The Audit Manual for the IPPs, published by the OPC, also discusses the status of guidelines and provides that 'in any privacy audit, the auditors may, at the discretion of the Privacy Commissioner, examine and report on the level of adherence to any such additional guidelines'.[48] Thus, while guidelines issued under s 27(1)(e) are not determinative, they are often highly persuasive.

Privacy code guidelines

44.27 Specific provision is made for the Commissioner to prepare and publish guidelines regarding privacy codes. These may assist organisations to develop or apply approved privacy codes; relate to the making of, and dealing with, complaints under approved privacy codes; or discuss matters the Commissioner may consider in deciding whether to approve a code or a variation of an approved code.[49] The OPC published *Guidelines on Privacy Code Development* in September 2001.[50] These Guidelines are binding in relation to complaint handling under a code but otherwise are advisory only.[51]

Power to issue binding guidelines

Tax file numbers

44.28 In addition to the Commissioner's powers to issue non-binding guidelines, the Commissioner can also issue 'binding' statutory guidelines under the *Privacy Act* and other Acts. For example, under s 17 of the *Privacy Act*, the Commissioner must issue guidelines concerning the collection, storage, use and security of TFN information.[52]

---

46 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 26. A similar approach is taken in the Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals* (2001), 25; Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), i.

47 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 3.

48 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5.

49 *Privacy Act 1988* (Cth) s 27(1)(ea).

50 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001). The OPC has undertaken to review the Code Development Guidelines: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 47.

51 See *Privacy Act 1988* (Cth) s 18BB(3)(A)(ii).

52 See also Ibid s 28(1)(a).

These guidelines are made binding by virtue of s 18, which prohibits a file number recipient from doing an act or engaging in a practice that breaches the guidelines.[53]

44.29 The OPC issued Tax File Number Guidelines in 1992 and it publishes an annotated version of the Guidelines (including all amendments as at March 2004) on its website.[54] The Commissioner has a general power to evaluate compliance with TFN guidelines and may investigate an act or practice of file number recipients that may breach the guidelines.[55] File number recipients can also be audited to ascertain whether records of TFN information maintained by the recipient are in accordance with the s 17 guidelines,[56] which are discussed below.

Medical Research Guidelines

44.30 The *Privacy Act* also invests the Commissioner with the power to approve guidelines issued by the NHMRC in relation to medical research and genetic information under ss 95, 95A and 95AA.[57] Once approved, these guidelines are binding.

Other Acts

44.31 The Commissioner is specifically given the power to formulate and issue binding guidelines under s 12 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and s 135AA of the *National Health Act 1953* (Cth).[58]

ALRC's view

44.32 The power to issue guidance is an important part of regulating a principles-based regime such as the *Privacy Act*. The Commissioner's function in 27(1)(e), as currently drafted, is broad enough to enable the Commissioner to issue guidance on a range of matters, particularly when read in conjunction with the Commissioner's powers to issue advice, promote an understanding of the NPPs and IPPs, and undertake education programs. Accordingly, the ALRC is not proposing any reform to the guideline function at this stage.

44.33 The ALRC proposes, however, that the language used in the Act should be changed to reflect more accurately the binding or non-binding nature of the guidelines issued. Non-binding guidelines should continue to be called 'guidelines', as they provide a voluntary guide on ways to achieve the outcome set by the relevant privacy principle, without directly compelling a particular course of action. In contrast, where the guidelines provide rules for compliance, a breach of which constitutes an interference with privacy, then they should be called 'rules'. This is consistent with the

---

53 A breach of these guidelines constitutes an interference with the privacy of the individual: Ibid s 13(b).
54 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
55 *Privacy Act 1988* (Cth) ss 28(1)(f), s 28(1)(b).
56 Ibid s 28(1)(e).
57 These guidelines are discussed further in Ch 58.
58 *Privacy Act 1988* (Cth) s 27(1)(p)–(pa).

ALRC's proposal that the Act be redrafted to achieve greater clarity.[59] This proposal will assist agencies and organisations to distinguish between guidelines that are merely advisory and those that operate as rules.

Proposal 44–2 The *Privacy Act* should be amended to reflect that where guidelines issued by the Privacy Commissioner are binding they should be renamed 'rules'. For example, the following should be renamed to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*:

(a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed *Tax File Number Rules*;

(b) Medicare and Pharmaceutical Benefits Programs Privacy Guidelines (issued under s 135AA of the *National Health Act 1953* (Cth)) should be renamed the *Medicare and Pharmaceutical Benefits Programs Privacy Rules*;

(c) Data Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth)) should be renamed the *Data Matching Program (Assistance and Tax) Rules*; and

(d) Guidelines for National Privacy Principles about genetic information should be renamed *Genetic Information Privacy Rules*.

Personal Information Digest

Background

44.34 The Commissioner has the function under s 27(1)(g) of maintaining and publishing annually, a record of 'the matters set out in records maintained by record-keepers in accordance with clause 3 of IPP 5'. Record keepers, in this context, are agencies. This record is known as the Personal Information Digest (Digest). The matters that must be included in the Digest are the:

- nature of the records of personal information kept by or on behalf of the record-keeper;
- purpose for which each type of record is kept;

---

59 See Proposal 3–2. Note that, as the ALRC proposes to abolish the existing ss 95 and 95A guidelines (see Ch 58), the ALRC has not included these guidelines in Proposal 44–2 (although if they remain, they should be renamed rules consistent with Proposal 44–2). This language is also consistent with the approach taken in *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 229.

- classes of individuals about whom records are kept;
- period for which each type of record is kept;
- persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
- steps that should be taken by persons wishing to obtain access to that information.

44.35 Currently, agencies provide their Digest entries to the OPC, which then makes them available on the OPC website.

Submissions and consultations

44.36 In IP 31, the ALRC asked whether the Digest is published in a useful manner, how it could be improved and whether the record itself is useful.[60] All of the submissions received by the ALRC that discussed the Digest recommended that it be changed in some way. For example, the Australian Government Department of Human Services submitted:

> The current arrangements are not very useful and are repetitive to prepare. Most agencies have adopted the use of websites to publish relevant information about record holdings. The websites in most cases contain much more information than was contemplated when the *Privacy Act 1988* was implemented.[61]

44.37 The OPC suggested that the manner of reporting the Digest may need to be changed and that the form of the Digest should be reviewed. In particular, the OPC suggested that it may be more appropriate for agencies to include the information currently reported to the OPC in the Digest entry on their websites or to report the updating of their Digest entry in their annual report, with the OPC overseeing compliance with these requirements. The OPC suggested that the form of the Digest should be reviewed, particularly in light of the OPC's suggestion that agencies develop a comprehensive privacy policy. If such a suggestion were taken up, the OPC considered it 'questionable' whether it would still be necessary for agencies to create a Digest entry.[62]

44.38 Other stakeholders thought the Digest was valuable, but that its utility could be improved. For example, the Australian Federal Police (AFP) submitted that the Digest 'is a useful document to collate the ways in which an agency collects, stores, and provides access to personal information as well as why the agency collects the

---

60 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–8.

61 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007. See also Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.

62 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

information'.[63] The AFP noted, however, that the Digest is based on a concept of hard copy published reports being the most reliable source of official information, and suggested that there may now be 'other ways for agencies to make this information available to citizens, for example through self publishing on agency websites in line with guidelines issued by the Privacy Commissioner'.[64]

44.39 It was also submitted that the Digest has the potential to provide a valuable research tool for academic inquiry, investigative journalism and Parliamentary scrutiny, but, to date, it has not been used as effectively as it could be.[65] It was suggested that the requirement to prepare a Digest be retained, but that accessibility to the Digest be improved, for example, by publishing it on the internet in searchable form and allowing other publishers to re-publish it with different forms of search facilities added. This would, it was said, 'make it easier to track the extent of use and interconnection of personal information'.[66] It was also suggested that the Commissioner should be given more scope to vary the amount of information an agency is required to disclose, and the power to require businesses to prepare a Digest entry.[67]

ALRC's view

44.40 The ALRC proposes that the general notification principles currently located in the IPPs and NPPs should be consolidated and simplified into a proposed 'Openness' principle.[68] The proposed principle would require an agency to produce a 'Privacy Policy' setting out the type of information currently required in the Digest entry, with some additions. The agency or organisation would be required to take reasonable steps to make its Privacy Policy available to an individual electronically, such as on its website, or in hard copy.[69]

44.41 This proposal, if implemented, would obviate any need for the current requirement to prepare a Digest entry. It would also mean that the corresponding obligation on the Commissioner to prepare the consolidated Digest could be removed.

44.42 The question remains, however, whether the OPC should have any corresponding obligation in relation to Privacy Policies—that is, to prepare and publish on its website a consolidated index of all Privacy Policies. The ALRC's preliminary view is that this is not necessary. It would be resource-intensive for the OPC to establish and maintain the register and it is not clear that there would be a benefit in so

---

63 Australian Federal Police, *Submission PR 186,* 9 February 2007.
64 Ibid.
65 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
66 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
67 Ibid; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
68 See Ch 21.
69 See Proposal 21–4.

doing, as it is unlikely to increase awareness of privacy policies more generally. As a number of stakeholders pointed out, publication of the Digest on the OPC website is an historical anomaly. In the current environment, individuals seeking an agency's Privacy Policy are more likely to go to the agency's website than look on the OPC website. The key concern is that Privacy Policies should be readily available to members of the public, which would be achieved by the requirement to make the Policies available without charge electronically or in hard copy.

Proposal 44–3 Following the adoption of Proposal 21–1 to require agencies to produce and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.

Privacy impact assessments

Background

44.43 Privacy impact assessments (PIAs) have been the topic of much discussion in recent reviews of the *Privacy Act* and in privacy commentary more generally. The term 'privacy impact assessment' is not defined in the *Privacy Act*, nor is there a requirement for the Commissioner, or for an agency or organisation, to undertake a PIA. There is, however, a related function vested in the Commissioner, which is to examine and advise on a proposed enactment.[70] While the Commissioner may produce a PIA as a result of such an examination, the term 'privacy impact assessment' has come to refer to a more formalised assessment conducted by the relevant agency or privacy consultant, rather than by the Commissioner.[71]

44.44 This section provides some background on the role of PIAs in a regulatory regime and draws on some international examples. It also considers submissions received by the ALRC on questions asked in IP 31 relating to when a PIA should be prepared and by whom.[72]

Definition

44.45 The OPC suggests that a PIA is an assessment tool that 'tells the story' of the project from a privacy perspective. It describes the personal information flows in a

---

70 *Privacy Act 1988* (Cth) s 27(1)(b). Privacy Commissioners in other Australian jurisdictions have similar powers to examine and advise on the privacy impacts of proposed legislation. See, eg, the *Information Privacy Act 2000* (Vic) s 58(1); *Information Act 2002* (NT) s 86(1)(f); *Information Act 2002* (NT) s 86(1)(f). See also *Human Rights and Equal Opportunity Act 1986* (Cth) ss 11(1)(e), 46C(1)(d); *Disability Discrimination Act 1992* (Cth) s 67(1)(i); *Sex Discrimination Act 1984* (Cth) s 48(1)(f).

71 See, eg, the Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006); New Zealand Government Privacy Commissioner, *Privacy Impact Assessment Handbook* (2007); Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments—a guide* (2004).

72 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 6–6, 6–7.

project and analyses the possible impact on privacy of those flows.[73] Others have suggested a PIA is 'an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'.[74]

44.46 It is suggested that PIAs are a form of proactive regulation that can help prevent privacy intrusive legislation or projects from being implemented. In a principles-based regulatory regime, PIAs can also help 'marry the discretion allowed under the Act with a degree of accountability to the public where a significant privacy erosion will be caused'.[75] In addition, a PIA may also help 'tackle wider privacy issues such as intrusion'[76] and are seen by many as one of the key ways to address the possible privacy impact (whether negative or positive) of new or developing uses of technology.[77]

44.47 The most significant benefits of a PIA are achieved when it is integrated into the decision-making process for the project.[78] It has been suggested that the PIA must take place 'during the development of proposals when there is still an opportunity to influence the proposal'.[79] In this way, a PIA is to be distinguished from a privacy compliance audit. While both are proactive compliance measures, the latter examines the information-handling practices of an auditee 'that are in place at the time, as opposed to future proposals that the auditee might be contemplating'.[80] A PIA, in contrast, focuses on future projects.

Status in Australia

44.48 As noted above, the Commissioner can prepare a PIA when exercising the function of examining and advising on proposed enactments. While the Commissioner can report to the Minister about a proposed enactment and *must* report if directed to do

---

73 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 4.

74 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61, 62. See also the definitions of PIAs in Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.1].

75 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61, 61.

76 Ibid, 61.

77 See eg, the Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005). See also B Stewart, 'Privacy Impact Assessment: Towards a Better Informed Process for Evaluating Privacy Issues Arising from New Technologies' (1999) 5 *Privacy Law and Policy Reporter* 147.

78 B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61. See also Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.3].

79 United Kingdom Government Information Commissioner's Office, *Evidence Submitted to the Home Affairs Committee Inquiry into 'The Surveillance Society?'* 23 April 2007, 6.

80 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 64. See also Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.7]; B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

so by the Minister,[81] the Minister is not required to obtain the OPC's advice in relation to proposed legislation or to act on any recommendations made by the OPC in a report to the Minister.[82] Similarly, there are no requirements in the *Privacy Act* for an agency to undertake a PIA. In the absence of a legislative directive, the OPC has said the incentive for doing a PIA comes from the fact that 'the success of an agency's project will depend in part on it complying with legislative privacy requirements and how well it meets broader community expectations about privacy'.[83]

44.49 To encourage agencies to undertake PIAs, the OPC produced a Privacy Impact Assessment Guide (PIA Guide), which provides detail on the nature, purpose and effect of a PIA. The PIA Guide contains modules for undertaking the PIA process. The PIA Guide notes that, while there is no formal role for the OPC in the development, endorsement or approval of PIAs, the OPC may be able to advise agencies on privacy issues arising throughout the assessment process.[84] The OPC often recommends that a department undertake a PIA as part of its advice on proposed enactments and policy submissions.[85] Departments sometimes conduct PIAs 'in-house' and often hire privacy consultants to conduct the PIA.

44.50 The OPC has not prepared a similar guide for organisations, although the use of PIAs in the private sector was discussed in the OPC Review. It was suggested that organisations should use the PIA process 'to assess and avoid privacy risks inherent in many large scale projects using new technologies'.[86] The OPC noted that it could encourage those that develop new technologies, and those that use such technology, to conduct a PIA for large-scale, high privacy risk projects.[87] Ultimately, the OPC did not recommend that organisations should be *required* to prepare, or obtain, a PIA. The OPC has subsequently noted that 'it considers that the best way for organisations and government agencies to avoid interferences with privacy is for them to use a [PIA] to

81 *Privacy Act 1988* (Cth) s 31. Currently, the relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

82 The Australian Government Department of the Prime Minister and Cabinet, *Legislation Handbook* (1999), [4.7(h)(vi)] provides that, in relation to legislative matters going before Cabinet, it is expected that the relevant department undertake other consultations in preparing the submission, including 'with the Privacy Commission [sic] if the legislation has implications for the privacy of individuals'.

83 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 4.

84 Ibid, 17.

85 See, eg, Australian Government Office of the Privacy Commissioner, *Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006*, 2; Office of the Privacy Commissioner, *Comments to the Attorney-General's Department on the Review of the Law on Personal Property Securities: Discussion Paper 1 Registration and Search Issues*, 1 February 2007, 3.

86 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 255–256.

87 Ibid, 256.

analyse the risks to privacy posed by new projects, technologies or rules and to address those risks before problems occur'.[88]

44.51 The Senate Committee privacy inquiry went further and recommended that the *Privacy Act* 'be amended to include a statutory [PIA] process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information'.[89] The Australian Government did not agree with the Senate's recommendation, noting that 'the Privacy Commissioner is developing a [PIA] process for use by agencies and considers that at this time a statutory process is not appropriate'.[90]

PIAs in other jurisdictions

Requirements on agencies

44.52 A number of jurisdictions require agencies to prepare a PIA in certain circumstances. The Canadian government was the first federal government to make PIAs mandatory.[91] Under the Canadian Government's Privacy Impact Assessment Policy, all federal departments and agencies must conduct a PIA 'for proposals for all new programs and services that raise privacy issues'.[92] Representatives of the Office of the Privacy Commissioner of Canada (Canadian Privacy Commissioner) must be involved at the earliest possible stage of the development of the PIA, and a copy of the PIA must be provided to the Canadian Privacy Commissioner and published on the internet.[93] The Canadian Privacy Commissioner's role is not to accept or reject projects, but 'to assess whether or not departments have done a good job of evaluating the privacy impacts of a project and to provide advice, where appropriate, for further improvement'.[94]

44.53 Some Canadian provinces also encourage or require PIAs.[95] In addition, the *E-Government Act* in the United States requires that a PIA be undertaken, reviewed by the Chief Information Officer of the agency and, if practicable, published, before an

88 S Jenner, 'The Impact of Computers on Privacy: A Virtual Story' (Paper presented at Striking A Balance: Computer Audit, Control and Security 2005 Conference, Perth, 23–26 October 2005).

89 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 5.

90 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006), 2–3.

91 G Greenleaf, 'Canada Makes Privacy Impact Assessments Compulsory' (2002) 8 *Privacy Law and Policy Reporter* 190. This policy took effect on 2 May 2002.

92 Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy* (2002).

93 Ibid.

94 S Bloomfield, 'The Role of the Privacy Impact Assessment' (Paper presented at Managing Government Information: 2nd Annual Forum, Ottawa, 10 March 2004), 3–4.

95 See, eg, the *Freedom of Information and Protection of Privacy Act 1996* RSBC c165 (British Columbia) s 69(5); *Health Information Act 2000* RSA c H–5 (Alberta) ss 46, 64, 70, 71.

agency develops or procures a new information system or initiates a new collection of personally identifiable information.[96]

Requirements on organisations

44.54 While there are precedents for requiring agencies to conduct PIAs, the ALRC is not aware of any jurisdiction that requires an organisation to conduct a PIA on new projects or developments. There has been, however, discussion about extending a PIA process to the private sector in the UK. The Office of the Information Commissioner (UK) (UK Information Commissioner) has proposed that PIAs be introduced 'to ensure public confidence in initiatives and technologies which could otherwise accelerate the growth of a surveillance society'.[97] The UK Information Commissioner argued that the introduction of PIAs would 'ensure organisations set out how they will minimise the threat to privacy and address all the risks of new surveillance arrangements before their implementation'.[98]

Submissions and consultations

44.55 In IP 31, the ALRC asked a number of questions about the role of PIAs in privacy regulation.[99] The ALRC received several submissions in response to these questions.

Statutory requirement on agencies

44.56 Several stakeholders expressed support for a statutory PIA process for proposed legislation or agency projects.[100] Others, however, opposed such a requirement.[101] The responses from those supporting a statutory PIA process ranged from support for empowering the Commissioner to carry out PIAs 'for all proposed Commonwealth legislation, or other proposed developments of agencies',[102] to a more qualified requirement for an agency to carry out a PIA where the legislation or project is likely to have an impact or significant impact on privacy. As an example of the latter

---

96 *E-Government Act of 2002* 2458 Stat 803 (US) s 208.

97 United Kingdom Government Information Commissioner's Office, 'Information Commissioner Calls for New Privacy Safeguards to Protect against the Surveillance Society' (Press Release, 1 May 2007).

98 Ibid.

99 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 6–6, 6–7.

100 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; CrimTrac, *Submission PR 158,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. See also New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

101 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; Confidential, *Submission PR 165,* 1 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Medicare Australia, *Consultation*, Canberra, 21 March 2007; Australian Taxation Office, *Consultation PC 135*, Canberra, 15 March 2007.

102 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

approach, the OPC supported the Senate Committee privacy inquiry recommendation that there be a statutory requirement for agencies to undertake a PIA for new projects or legislation that significantly impacts on the collection or handling of personal information.[103] The OPC suggested that, if a mandatory scheme is adopted, it should include a set of criteria to establish when a PIA is required.[104]

44.57 The Office of the Information Commissioner Northern Territory also supported a more qualified statutory requirement to prepare PIAs. It submitted that agencies should be required to consult with the OPC in relation to any legislation or proposal that raises privacy issues, and the OPC should be permitted to 'consider the need for a PIA, discuss the issue with the agency, and direct that an assessment be undertaken if necessary'.[105]

44.58 In contrast, the AFP did not believe that 'legislating to require a privacy impact assessment for the development of Commonwealth legislation is necessary'. It suggested that 'consideration of the impact of a range of competing interests, including privacy, is part of the policy approval and drafting stages of the development of legislation'.[106] The Insurance Council of Australia suggested that privacy impacts would not be relevant in a majority of situations and, where there is a potential privacy issue in relation to the introduction of new legislation or regulation, 'this could and should be simply built into the regulatory impact statement'.[107]

44.59 Numerous stakeholders also argued that imposing a statutory obligation on agencies to prepare PIAs was unnecessary, would be onerous, and is being done when required in any event. For example, the Australian Taxation Office (ATO) argued that requiring a PIA for all projects would impose a significant workload on agencies like the ATO, which handle a large volume of personal information. It submitted that it would favour 'voluntary use of PIAs for appropriate projects'. If a statutory requirement were introduced, the ATO submitted that it should only be for 'projects that will have a significant impact on the collection, use or data matching of personal information'.[108]

44.60 There was also a strong consensus in consultations that a statutory PIA requirement would be difficult to implement. Two main reasons were highlighted: the broad spectrum of circumstances in which privacy will be seen as an issue; and the large amount of personal information handled by agencies. It was also suggested that a

---

103 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

104 The OPC gave the Canadian criteria as an example: Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy* (2002).

105 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. See also Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007.

106 Australian Federal Police, *Submission PR 186,* 9 February 2007.

107 Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

108 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

statutory requirement would be seen as an administrative hurdle to get over rather than facilitating the minimisation of a project's impact on privacy.

Statutory requirement on organisations

44.61 The majority of stakeholders that commented on this issue opposed any requirement on organisations to conduct PIAs.[109] AAMI suggested that 'the law and its regulators are seen to be a stakeholder in any project management process and are therefore included in any stakeholder analysis'. It suggested that there appears to be little value in requiring organisations to prepare PIAs and it would 'simply add expense and another layer of "compliance" whilst the final outcome for customers would be the same (if not somewhat delayed)'.[110] The Australian Government Department of Employment and Workplace Relations (DEWR) submitted that there was 'no compelling case' to require the private sector to undertake PIAs and that, in any event, any organisation that undertakes a project or development will have to comply with the relevant privacy principles.[111]

44.62 The OPC noted that many projects undertaken by organisations would benefit from a requirement that PIAs be conducted during the development and implementation phases of such projects. The OPC did not support, however, imposing a statutory obligation on organisations to undertake PIAs for new projects or developments, believing that 'greater consumer choice in the private sector enables individuals to choose to interact with businesses with good privacy practices'.[112] It suggested instead that organisations should be encouraged to undertake PIAs for large-scale projects involving a high risk to privacy.[113]

44.63 The Office of the Information Commissioner Northern Territory submitted that organisations might benefit from a similar approach to that which it proposed for agencies. While the Information Commissioner noted that this approach would have resource implications for the OPC, it concluded that 'organisations should be encouraged to consult with the OPC in relation to major initiatives, and the option should remain for the OPC to become involved to the extent resources will allow'.[114]

44.64 In contrast, the Australian Privacy Foundation supported a requirement for organisations undertaking 'major personal information handling projects' to prepare

---

109 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; AAMI, *Submission PR 147,* 29 January 2007.

110 AAMI, *Submission PR 147,* 29 January 2007.

111 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

112 The notion of customer choice in a commercial context compared to lack of choice and often absence of consent when dealing with government agencies was part of the justification for introducing the mandatory PIA policy in Canada: S Bloomfield, 'The Role of the Privacy Impact Assessment' (Paper presented at Managing Government Information: 2nd Annual Forum, Ottawa, 10 March 2004), 2.

113 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

114 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

and publish a PIA before the organisation makes the decision to proceed with the project.[115]

Responsibility for conducting the PIA

44.65 In IP 31, the ALRC asked who should be involved in, and bear the cost of, preparing PIAs.[116] The majority of stakeholders suggested that the agency or organisation responsible for the project should prepare (or arrange for a third party to prepare) the PIA.[117] The OPC explained:

> The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts. Given that the agency or organisation's compliance with the *Privacy Act* is the responsibility of that agency or organisation, the Office considers that the conduct of any PIA should be the responsibility of the particular agency or organisation.[118]

44.66 The responses in relation to costs seemed to depend on whether the requirement to prepare the PIA was mandatory or voluntary. The Australian Privacy Foundation, which supported a mandatory scheme, submitted that the cost of the assessment should be borne by the proponent of the project.[119] The ATO submitted that the responsible agency generally should bear the cost, but that if the obligation was mandatory, consideration should be given to the resources involved and whether additional funding is required.[120]

Oversight and accountability

44.67 The ALRC also asked in IP 31 who should be entitled to view the results of a PIA, and what role the Commissioner should play in overseeing a requirement to prepare PIAs.[121] A number of stakeholders called for PIAs to be made publicly available.[122] While encouraging the publication of PIAs (such as in the PIA Guide), the OPC acknowledged that PIAs are essentially internal working documents designed to

---

115 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. A similar suggestion was made in Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

116 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–7(a), (c).

117 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Taxation Office, *Submission PR 168,* 15 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. The Australian Privacy Foundation submitted that PIAs could be undertaken either in-house, by the Privacy Commissioner, or by external consultants: Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

118 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. Similar reasons were given in Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

119 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. Similar comments were made in Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

120 Australian Taxation Office, *Submission PR 168,* 15 February 2007.

121 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–7(b), (d).

122 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

assist agencies to make good privacy decisions and, therefore, it is critical that the PIA process be 'unfettered by concerns regarding poor publicity'.[123] As such, the OPC appreciated there may be circumstances where agencies or organisations may not wish to publish their PIA in full.[124]

44.68 The OPC suggested that some kind of accountability mechanism should be included in the *Privacy Act* if a statutory requirement for PIAs to be conducted is introduced. This could be achieved by requiring agencies to include a report of PIAs undertaken in their annual report, or giving the Commissioner the function of monitoring PIAs undertaken—for example, by requiring that the Commissioner be provided with an opportunity to comment on PIAs produced under any mandatory requirement.[125] The Office of the Information Commissioner Northern Territory submitted that the OPC should have the power to approve the terms of reference for the PIA and review and comment on the assessment,[126] and the ATO suggested that the Commissioner provide clear guidelines and provide resources to assist agencies as required.[127]

Options for reform

44.69 There is general recognition of the value and benefits of conducting PIAs in relation to projects and developments of agencies, and, to a lesser extent, organisations. As a proactive regulatory tool, PIAs help identify privacy impacts and can prevent future problems. PIAs also help to build privacy compliance into the culture and practices of agencies and organisations, which is consistent with the OPC's overall approach to facilitating compliance with the *Privacy Act*.[128]

44.70 Having regard to those benefits, the ALRC is of the view that PIAs should be given some legislative underpinning in the *Privacy Act*. This could be done by either:

- amending the *Privacy Act* to include a requirement to prepare a PIA for proposed projects and developments that significantly impact on the handling of personal information; or

- encouraging the preparation of PIAs and empowering the Commissioner to direct the preparation of a PIA where the Commissioner thinks a project or

123 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
124 Ibid. A similar approach was taken in Australian Taxation Office, *Submission PR 168,* 15 February 2007.
125 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
126 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007. See also Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.
127 Australian Taxation Office, *Submission PR 168,* 15 February 2007. See also Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.
128 See, eg, Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001). See also Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.2].

development is likely to have a significant impact on the handling of personal information.

44.71 In both situations, the Commissioner could review and comment on the PIA produced and could report to the Minister on non-compliance. If necessary, the Commissioner could seek an injunction from the Federal Court to stop a project from being implemented if he or she believed it breached the *Privacy Act*.[129] Both of these options could be restricted to agencies, or be extended to organisations as well.

ALRC's view

44.72 The ALRC's view is that the second option is preferable at this stage. Agencies and organisations should be encouraged to conduct PIAs for new projects and developments, and the OPC should educate agencies and organisations on the value of PIAs and the process involved in conducting a PIA.[130] This encouragement and education should be supported by a power vested in the Commissioner to direct the preparation of a PIA and for the Commissioner to report to the Minister on non-compliance with such a direction. The relevant agency or organisation should prepare (or obtain) the PIA, as compliance with the Act is its responsibility and the project or development is its concern. The OPC should continue to review and provide guidance and advice on the PIA process, to ensure it adequately addresses and resolves privacy issues.[131]

44.73 The ALRC includes organisations in this proposal, as many new projects or developments undertaken by organisations would benefit from being subject to a PIA to ensure that the privacy risks are assessed and adequately managed in the design and implementation of the project. Organisations are often at the forefront of development and utilisation of new and developing technologies. While there may be an element of customer choice involved with organisations, this can be removed where the use of technologies is not disclosed to customers, or where it is so widespread across an industry that most companies of a comparable nature utilise the technology. It is also important that privacy compliance continue to be built into organisational practice, rather than be 'bolted on' at the end.[132]

44.74 A power to direct the preparation of a PIA should not place as large a compliance burden on agencies and organisations as a mandatory scheme, but rather seek to strengthen the existing voluntary regime. It is envisaged that the power to direct

---

129 See *Privacy Act 1988* (Cth) s 98.

130 In relation to terminology, the ALRC continues to adopt the definition of 'project' in the PIA Guide, where it is used to refer to any proposal, review, system, database, program, application, service or initiative that includes the handling of personal information: Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 3. The ALRC notes that a project could be a new development or a new policy proposal, and a project may be implemented by legislation or administratively.

131 This is consistent with the approach recommended in B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

132 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) United Kingdom Government Information Commissioner's Office, [45.1.2].

would be used primarily in two circumstances. First, it could be used where the OPC currently recommends that a PIA be undertaken, as part of its policy advice on a proposal or bill. Rather than being limited to 'recommending', the OPC would have the flexibility of directing, where appropriate, the agency to prepare the PIA. Secondly, it could be used where there has been some publicity about a project or development, or a complaint, inquiry or tip-off, and the OPC believes the project or development may have a significant impact on the handling of personal information.

44.75 Monitoring compliance with a direction to prepare a PIA should be less onerous and more manageable than monitoring compliance with a mandatory scheme, and the power to report non-compliance to the Minister should have a valuable deterrent effect. As part of the Commissioner's auditing functions, the Commissioner would also be able to assess the extent to which an agency or organisation complies with the voluntary PIA guide, which may alert the Commissioner to keep a closer watch on agencies or organisations that do not appear to be conducting PIAs where appropriate.[133] If a project raised serious privacy concerns, the Commissioner could apply to the Federal Court or the Federal Magistrates Court for an injunction to stop the agency or organisation from implementing the project, pending the preparation of the PIA and the review of that assessment by the OPC.[134]

Guidance

44.76 Consistent with the approach taken with agencies, the ALRC proposes that the OPC produce a PIA guide tailored to the needs of organisations. Such a guide should help educate organisations on the value of a PIA, the process involved, and the assistance that the OPC can give during the process of conducting a PIA. The OPC should also include guidance in the respective PIA guide on what constitutes a 'significant impact on the handling of personal information' and the circumstances in which the Commissioner may exercise the power to direct that a PIA be undertaken. These circumstances could draw on the examples put forward by Blair Stewart,[135] including where: the project or development involves a new technology or the convergence of an existing technology; the use of a known privacy intrusive technology in a new circumstance; or a major endeavour or change in practice that has obvious privacy risks.[136]

44.77 The PIA guide should also clarify the OPC's expectations in relation to preparing PIAs. In particular, there may be value in making it clear that there is a prima facie obligation on agencies and organisations to prepare a PIA for new projects or developments that may have a significant impact on the handling of personal

---

133 The OPC already monitors compliance with voluntary guidelines, such as the Data-Matching Guidelines, even though they are not binding. See Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 9.

134 See *Privacy Act 1988* (Cth) s 98.

135 Assistant Commissioner (Policy), Office of the Privacy Commissioner New Zealand.

136 See B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61.

information, and if the agency or organisation decides not to conduct a PIA, it should inform, and justify the decision to, the OPC.[137]

Proposal 44–4 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and

(b) report to the Minister an agency or organisation's failure to comply with such a direction.

Proposal 44–5 The Office of the Privacy Commissioner should develop Privacy Impact Assessment Guidelines tailored to the needs of organisations.

Compliance powers

44.78 Regulatory theorists suggest that a critical part of ensuring compliance with a regulatory regime is to monitor and enforce implementation of the regime by the regulated entities.[138] The Commissioner's functions in monitoring compliance with the *Privacy Act* include: conducting audits and examining records; receiving, investigating and resolving privacy complaints; enforcing the Act through determinations, injunctions and federal court proceedings; and determining that certain acts or practices will not be taken to breach the Act where there is a substantial public interest in doing so.

44.79 The Commissioner's complaint handling and enforcement powers are discussed in the next two chapters. This part of the chapter focuses on the Commissioner's auditing functions, including self-auditing and public interest determinations.

137 This is analogous to the approach taken in the Australian Stock Exchange Listing Rule 4.10. This rule requires an entity to disclose the extent to which they have followed best practice recommendations and if it has not followed all recommendations, the entity must identify the recommendations that have not been followed and give reasons for not following them. See Australian Stock Exchange, *Listing Rules—Chapter 4: Periodic Disclosure* (2005) <www.asx.com.au/ListingRules/chapters/Chapter04.pdf> at 31 July 2007, [4.10.3].

138 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 535; F Cate, 'The Failure of Fair Information Practice Principles' in J Winn (ed) *Consumer Protection in the Age of the 'Information Economy'* (to be published 2007) Ch 14.

Audit functions

Background

44.80 The Commissioner has a number of functions under the *Privacy Act* to audit compliance. The OPC describes an audit as 'a snapshot of personal information handling practices in relation to an agency or organisation program at a certain time and in a particular location'.[139] An audit involves a systematic inspection and review of an agency and organisation, to obtain evidence to enable the Commissioner to assess the extent to which records are maintained in accordance with various provisions of the Act.[140]

44.81 The spot audit and examination functions conferred on the Commissioner are divided between the IPPs, TFN information and credit reporting provisions, and include:

- auditing records of personal information maintained by agencies to ascertain whether they comply with the IPPs;[141]
- auditing particular acts and practices of agencies in relation to personal information, if the acts or practices are prescribed by regulations;[142]
- auditing records of TFN information maintained by file number recipients to ascertain whether they comply with the TFN Guidelines;[143]
- monitoring the security and accuracy of TFN information kept by file number recipients;[144]
- examining the records of the Commissioner of Taxation to ensure he or she is not using TFN information for unauthorised purposes and is taking adequate measures to prevent the unlawful disclosure of such information;[145]
- auditing credit information files maintained by credit reporting agencies and credit reports possessed by credit providers or credit reporting agencies to

---

139 Office of the Privacy Commissioner, *Audit Information* (2007) <www.privacy.gov.au/government/audits/index.html> at 31 July 2007.

140 Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), 5. See also Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995); Office of the Privacy Commissioner, *Privacy Audit Manual—Part III (Credit Information)* (1995).

141 *Privacy Act 1988* (Cth) s 27(1)(h).

142 Ibid s 27(1)(ha).

143 Ibid s 28(1)(e).

144 Ibid s 28(1)(h).

145 Ibid s 28(1)(d).

ascertain whether they comply with the *Credit Reporting Code of Conduct* and Part IIIA of the *Privacy Act*;[146] and

- examining the records of credit reporting agencies and credit providers to ensure they are not using personal information contained in the files or reports for unauthorised purposes and are taking adequate measures to prevent the unlawful disclosure of such information.[147]

44.82 The number of audits carried out each year by the OPC has 'varied over the life of the *Privacy Act* depending on the nature of privacy complaints and other priorities of the Office'.[148] The OPC notes in its 2005–06 Annual Report that:

> In 2005-06 the Office only undertook audits where it had received specific funding to do so. This is consistent with the approach taken by the Office since 2002-03 when the Commissioner decided to redirect the Office's resources as a result of the significant increase in complaint numbers.[149]

Audits of organisations

44.83 Organisations are subject to audit by the Commissioner under functions associated with the TFN and credit reporting provisions, as discussed above. There is no general power to 'spot audit' the privacy compliance of organisations. If an organisation requests it, however, the Commissioner has power to examine the records of personal information maintained by the organisation, for the purpose of ascertaining whether the records are maintained in compliance with either an approved privacy code or the NPPs, as applicable.[150] As at the date of the OPC Review, the Commissioner had not conducted any audits under this power.[151]

Previous inquiries

44.84 Several stakeholders in the OPC Review and Senate Committee privacy inquiry submitted that the NPPs should be amended to confer an audit power on the Commissioner.[152] One participant in the OPC Review commented that if the Commissioner had audit powers, 'we might be able to convince our boards to comply

---

146 Ibid s 28A(1)(g).

147 Ibid s 28A(1)(j). Note, the Commissioner also has a monitoring role under the *Telecommunications Act 1997* (Cth), which is discussed further in Part J.

148 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 43.

149 Ibid, 43. An example of specific funding arrangements is the OPC's memorandum of understanding with the ACT Government: Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 43.

150 *Privacy Act 1988* (Cth) s 27(3).

151 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 157.

152 See Ibid, 145; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.35], [6.39].

[with the *Privacy Act*]'.[153] Others expressed the view that an extended audit power is necessary to maintain public confidence in the Commissioner's role.[154]

44.85 The OPC Review did not, however, recommend that the Commissioner be given the power to audit organisations. While recognising that a private sector audit power may increase community confidence in the efficacy of the *Privacy Act* and give the OPC additional power to identify systemic issues and to monitor responses, the OPC concluded that it would have resource implications and may be a more appropriate role for private consultants to perform.[155] The OPC Review recommended instead that it would 'consider promoting privacy audits' by organisations, such as by providing information on the value of auditing as evidence of compliance in the event of complaints, and by developing and providing privacy audit training.[156] In contrast, the Senate Committee privacy inquiry urged the introduction of OPC private sector auditing powers.[157]

Private sector audits in other jurisdictions

44.86 The Canadian Privacy Commissioner has power to conduct audits of private sector organisations under the *Personal Information Protection and Electronic Documents Act* 1985 (Canada).[158] This Act provides that the Canadian Privacy Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organisation if the Commissioner has reasonable grounds to believe that the organisation is contravening particular provisions of the Act.[159]

44.87 The UK Information Commissioner's power to conduct audits on private sector organisations has a similar limitation to that of the OPC—it can only be done with the organisation's consent.[160] The UK Information Commissioner has recently called for stronger powers to allow the Information Commissioner's Office to carry out inspections and audits of organisations without the organisation's consent.[161] The UK Information Commissioner argued that the requirement for consent 'fetters' the power

---

153 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 133.

154 Ibid, 145.

155 Ibid, 157.

156 Ibid, rec 39.

157 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.56].

158 The Canadian Privacy Commissioner also has power to conduct audits on government bodies: *Privacy Act* RS 1985, c P-21 (Canada) ss 37–39.

159 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada). Guidance on the circumstances that may lead to an audit is provided in Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations: Your Privacy Responsibilities—Canada's Personal Information Protection and Electronic Documents Act* (2004) <www.privcom.gc.ca/information/guide_e.asp> at 31 July 2007, 25.

160 *Data Protection Act 1998* (UK) s 51(7).

161 United Kingdom Government Information Commissioner's Office, *Evidence Submitted to the Home Affairs Committee Inquiry into 'The Surveillance Society?'* 23 April 2007, 7.

to conduct audits and inspections and 'limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance'.[162]

Submissions and consultations

44.88 In IP 31, the ALRC asked what powers the Commissioner should have to audit agencies and organisations.[163] Some stakeholders commented that the Commissioner's audit powers were appropriate and an important tool.[164] The OPC considered privacy audits 'are a key method for determining the extent of compliance with the *Privacy Act* and are an important educative tool'.[165] In relation to private sector auditing, submissions either favoured extending the Commissioner's power without limitation (similar to the power to audit agencies) or extending it with some qualification—for example, restricting its use to where there is evidence of some widespread or systemic issues in the organisation or industry.

In support of a general private sector audit power

44.89 A number of stakeholders supported the extension of a general audit power to the private sector.[166] For example, the Australian Privacy Foundation suggested that the audit power should be extended to organisations, 'where reliance on complaints to detect non-compliance is arguably even less effective than in the public sector'.[167] The Centre for Law and Genetics described the audit power as a 'crucial issue' and suggested that:

> If the approach of general guidance principles and industry codes is to have any public credibility and practical effectiveness, the [Privacy Commissioner] must have genuine powers to audit agencies and organisations. As the approach aims to develop a co-operative model, the OPC should have powers that require actions by the agency or organisation to address the problem *before* a mandatory audit. The power to carry out unannounced spot audits should be restricted to serious cases.[168]

In support of a qualified private sector audit power

44.90 Several stakeholders preferred a more qualified private sector audit power—that is, one that can only be exercised following certain triggers. The OPC, while reiterating its concerns about resourcing, noted that the Commissioner's current audit functions 'do not provide the flexibility to identify other areas or practices that may require

---

162 Ibid, 7.

163 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–9.

164 Australian Federal Police, *Submission PR 186,* 9 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

165 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

166 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005, as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

167 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

168 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

particular scrutiny through privacy audits undertaken by the Office'.[169] Accordingly, the OPC suggested that the *Privacy Act* be amended to give the Commissioner a power to audit organisations where the Commissioner has reasonable grounds to believe that the organisation is engaging in practices that: pose new and significant risks to the personal information they hold; or contravene the privacy principles in the Act or a commitment made in response to a complaint or own-motion investigation. A reasonable belief of the first point could be established by community concern regarding the emergence of a new technology in the private sector, such as the use of biometrics. A reasonable belief of the second point could be 'established through further complaints or observance of continuing non-compliant practice following an investigation into a complaint or an own-motion investigation'.[170]

44.91 The OPC noted that its audit activities, while part of a compliance framework, serve primarily an educative function and that, just as there are no sanctions attached to poor privacy practices identified in a credit reporting or TFN audit, it does not propose that sanctions be introduced in respect of an NPP audit.[171] The OPC noted that it

> anticipates that it is likely that an NPP audit power as described would be infrequently used. However, where appropriate, it would allow the Office to expand on its current own motion investigation activities to formally interrogate the general information handling practices of an organisation and work with the organisation to address any privacy risks or ongoing privacy issues identified.[172]

44.92 AAMI and the Investment and Financial Services Association (IFSA) also supported a limited private sector audit power. AAMI submitted that the Commissioner should be able to audit organisations if there have been 'systemic issues identified and the OPC is of the view that the business is continuing to fail to comply with the *Privacy Act*, despite the use of infringement notice/enforceable undertakings'.[173] IFSA submitted that its member organisations are already subject to ongoing regulatory audits by APRA and ASIC and would 'resist the concept of random compliance audits by yet another government body'.[174] IFSA submitted that its industry's history of good levels of compliance in handling personal information, which it says is evidenced by the low level of complaints, suggests that random audits are not necessary. IFSA also stated, however, that it would not object to 'audits based on reasonable grounds such as systemic issues'.[175]

---

169 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

170 Ibid.

171 The audit manuals produced by the OPC confirm the educative and advisory focus of audits: see, eg, Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), [1.6.3–1.6.4]. Note also that the educative focus is emphasised in Office of the Privacy Commissioner, *Audit Information* (2007) <www.privacy.gov.au/government/audits/index.html> at 31 July 2007.

172 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

173 AAMI, *Submission PR 147,* 29 January 2007.

174 Investment and Financial Services Association, *Submission PR 122,* 15 January 2007.

175 Ibid.

Resourcing

44.93 Some of the stakeholders who commented on the Commissioner's audit power also addressed the related issue of resourcing. There was some consensus that the audit power is valuable (whether or not extended to the private sector) and the Commissioner should be resourced sufficiently to be able to exercise it effectively.[176] Several stakeholders also noted specifically that resourcing would need to be increased if the audit power were extended to the private sector.[177]

ALRC's view

Audit function

44.94 The OPC's audit functions are an important part of its compliance activities. It is one of the few proactive regulatory tools vested in the OPC, in that it allows the Commissioner to monitor an agency or organisation's compliance with the *Privacy Act* before, and in the absence of, evidence of non-compliance, with the aim of preventing such non-compliance occurring in the future. It also allows the Commissioner to identify systemic issues and bring about systemic change, and to use information gathered in an audit to target educational materials and programs.[178]

44.95 In relation to private sector audits, there is some consensus among stakeholders that the Commissioner should have a power to audit organisations to assess compliance with the NPPs. The difference of opinion arises as to when the Commissioner should be able to exercise the power, and, in particular, whether the Commissioner should have a wide or a qualified audit power.

44.96 In the ALRC's view, the real value in audits lies in their proactive nature—they can be used to take a snapshot of the level of compliance in an agency or organisation or across an industry. The presence of an audit power can act as an important preventative measure, as 'the existence of the audit functions and programs encourages organisations subject to the Act to take compliance seriously'.[179] The ALRC's preliminary view, therefore, is that the power to audit organisations should not be restricted to situations where there are reasonable grounds to believe that the organisation is engaging in practices that pose new and significant risks or contravene the privacy principles or a commitment made in a settlement. Rather, the Commissioner should be empowered to spot audit the levels of compliance in

---

176 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

177 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; National Association for Information Destruction, *Submission PR 133,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

178 See Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 50.

179 See Office of the Privacy Commissioner, *Audit Information* (2007) <www.privacy.gov.au/government/audits/index.html> at 31 July 2007.

organisations more generally, as she is currently empowered to do in relation to agencies.

44.97 This approach is consistent with the current position of audits on the compliance spectrum—that is, they are considered primarily educative and there are generally no penalties attached to a poor privacy audit (unless there is some evidence of deliberate wrongdoing).[180] It may complicate the overall enforcement approach of the OPC if the OPC could undertake an audit to address situations where there is a reasonable belief that the organisation is engaging in non-compliant acts or practices. The ALRC believes that the Commissioner's own motion investigation power provides a more appropriate mechanism for such situations.

44.98 Audits could also have a role to play following a complaint settlement or determination, or the issuance of a compliance notice.[181] In particular, it may be valuable for the OPC to undertake pre-emptive spot audits to assess whether the organisation is abiding by the terms of the settlement, determination or compliance notice—or to require the organisations themselves to undertake such audits. This is analogous to an undertaking under s 87B of the *Trade Practices Act 1974* (Cth), which may include agreement by the company to have its compliance program independently audited for a number of years and provide the audit report to the Australian Competition and Consumer Commission (ACCC).[182] The ALRC does not believe that auditing should be limited to where the Commissioner believes the organisation is contravening a commitment made in resolution of a complaint or own motion investigation. Such a case may require a more serious response than an educative audit—an investigation could be undertaken or enforcement action could be instituted in the federal courts.

Audit manuals

44.99 If the Commissioner's audit function were expanded to include private sector audits, the ALRC believes that it would be valuable for the OPC to develop an audit manual for organisations (or amend the existing IPP Manual) to provide further detail on the processes involved in an audit. In addition, the audit manuals should clarify when the results of an audit will be used in an educative and collaborative manner, and when they may lead to sanctions. Audit manuals should be updated to reflect the OPC's current expectations as to the levels of compliance to be achieved by agencies and organisations.[183]

---

180 The TFN Manual explains that, if any evidence of deliberate breaches of the Guidelines are detected by the auditors, the matter will be referred to the relevant authority for consideration of further action: Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995), 4.

181 See Proposal 46–1.

182 Australian Competition and Consumer Commissioner, *Section 87B of the Trade Practices Act: A Guideline on the Australian Competition and Consumer Commission's Use of Enforceable Undertakings* (1999), 7.

183 The ALRC notes that the manuals reflect the Commissioner's expectations at the time the Manuals were published, which may now be out-dated. For example, the Credit Reporting Manual sets out that, as credit

Consolidating audit functions

44.100 Consistently with the ALRC's proposal that the *Privacy Act* be amended to achieve greater logical consistency, simplicity and clarity,[184] the audit functions of the Commissioner should be consolidated. Given the ALRC's proposal to introduce the Unified Privacy Principles (UPPs), audit functions for agencies and organisations could be combined and could include TFN and credit reporting auditing. References to agencies or organisations would include agencies or organisations in their capacity as file number recipients and as credit providers or credit reporting agencies, as applicable.

Proposal 44–6 The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct audits of the records of personal information maintained by organisations for the purpose of ascertaining whether the records are maintained according to the proposed Unified Privacy Principles (UPPs), Privacy Regulations, Rules and any privacy code that binds the organisation.

Self-auditing

Background

44.101 A possible alternative or addition to the Commissioner's power to conduct audits is a requirement on agencies or organisations to undertake self-auditing.[185] The *Corporations Act 2001* (Cth) model of financial reporting and audits was suggested as a possible model. That model includes an obligation on corporations to self-audit, to report periodically to the Australian Securities and Investments Commission (ASIC), and to be subject to audit by ASIC. By analogy, organisations subject to the federal privacy regime could be required to self-audit privacy compliance and, if requested by the OPC, report to the Commissioner on their compliance.[186] The Commissioner could then audit such organisations as the Commissioner chooses, without being required to audit every organisation.

44.102 There is some movement towards self-auditing for privacy in the United States. While some regimes, particularly those relating to the private sector, 'do not

---

reporting provisions have 'only' been in force since 1992, the 'Commissioner has taken the view that credit providers should be given the benefit of the doubt where instances of breach are detected. In any case only in clearly culpable circumstances would further action be taken'. See Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995), [1.6.1–1.6.2].

184 See Proposal 3–2.

185 M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006. See also M Crompton, 'Respecting People, Their Individuality and Their Personal Information: The Key to Connected Government, Now and in the Future' (Paper presented at Public Services Summit, Stockholm, 9 December 2005). See also Baycorp Advantage, *Consultation PC 2*, Sydney, 24 February 2006.

186 A stakeholder to the Senate Committee privacy inquiry suggested a 'self-audit-self-regulatory process' as a more efficient way to deal with complaints: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.21].

explicitly require the formal conduction and report of an audit, auditing is generally necessary in order to be in full compliance'.[187]

Submissions and consultations

44.103 In IP 31, the ALRC asked whether organisations and agencies should be required to self-audit periodically to ensure and to demonstrate compliance with the *Privacy Act*.[188] Submissions were divided between those in support of a mandatory self-audit scheme and those who opposed such a scheme.

44.104 A number of stakeholders supported a general requirement to self-audit periodically as part of a compliance program,[189] with one suggesting that audit findings be published.[190] Several stakeholders who supported the introduction of self-auditing requirements noted they already conduct these audits periodically.[191] The NSW Disability Discrimination Legal Centre supported a self-audit requirement and stated that 'regular auditing has proved to be a powerful tool in ensuring both awareness of, and compliance with, principles of practice in areas of Equal Employment Opportunity, Freedom of Information, and Occupational Health and Safety'. There was, it said, 'no reason to believe that auditing would not function in the same way in the privacy context'.[192]

44.105 The Fundraising Institute of Australia welcomed the requirement to self-audit privacy compliance 'as it will serve to strengthen the role of the Privacy Principles, as well as guide both business and consumers in their choices of business and transactional interactions'.[193] It noted, however, the difficulty of self-auditing in the complex and multi-layered legislative environment that currently exists and urged strongly that uniform privacy principles be implemented before any legislative requirement to self-audit is introduced. It also suggested that guidelines for self-audits be clear and not overly burdensome.[194]

44.106 On the other hand, the OPC submitted that a self-audit requirement 'may not be the most appropriate way to facilitate better privacy compliance'.[195] While recognising there may be a greater role for the OPC in assisting organisations to

---

187 C Easter, 'Auditing for Privacy' (2006) 2 *I/S: A Journal of Law and Policy for the Information Society* 879, 880.

188 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–10.

189 CrimTrac, *Submission PR 158,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006; Baycorp Advantage, *Consultation PC 2*, Sydney, 24 February 2006.

190 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

191 Australian Federal Police, *Submission PR 186,* 9 February 2007; CrimTrac, *Submission PR 158,* 31 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

192 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

193 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.

194 Ibid.

195 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

undertake self-audits, it suggested that a mandatory scheme may put a disproportionate compliance burden on businesses that are not significant data-holders. It would also require monitoring by the OPC, which, given the huge number of organisation and agencies that are subject to the *Privacy Act*, would have intensive resource implications. For these reasons, the OPC considered that it would be more appropriate and efficient for a targeted private sector audit function to be introduced in the *Privacy Act* rather than a requirement to self-audit.

44.107 Several stakeholders argued that there was no evidence to indicate systemic problems with compliance that would justify introducing a requirement to self-audit.[196] These stakeholders also pointed to the significant cost of auditing, with one suggesting that 'any benefit gained from auditing procedures is disproportionate to the burden placed on organisations'.[197] Stakeholders were more supportive of the OPC Review's suggestion that the OPC provide information to organisations about the value of auditing.[198]

44.108 Some stakeholders discussed the possibility of OPC recognition for good compliance with the *Privacy Act*, similar to the idea of the privacy logo raised in the OPC Review.[199] For example, while not supporting a legislative requirement to self-audit, Telstra submitted that it would support action on the part of the OPC to recognise organisations that have taken significant steps to comply with their privacy obligations, for example, by way of an OPC 'seal of approval' that could be used by an organisation on its website.[200] Other stakeholders suggested that the OPC could provide a user-pays audit service whereby organisations that are found to comply can get a 'tick in the box' for good compliance.[201] An alternative suggestion was to establish a certification program, where self-auditing and spot auditing are part of the certification process.[202]

ALRC's view

44.109 The ALRC agrees with the comments made by the Fundraising Institute of Australia that instituting a self-audit requirement at this time would be premature. Before such a requirement can be considered, there needs to be uniformity in the privacy regimes across Australia.[203]

---

196 Telstra, *Submission PR 185,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; AXA, *Submission PR 119,* 15 January 2007.

197 Law Council of Australia, *Submission PR 177,* 8 February 2007. See also Telstra, *Submission PR 185,* 9 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007.

198 Law Council of Australia, *Submission PR 177,* 8 February 2007; UNITED Medical Protection, *Submission PR 118,* 15 January 2007

199 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 111.

200 Telstra, *Submission PR 185,* 9 February 2007.

201 D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

202 National Association for Information Destruction, *Submission PR 133,* 19 January 2007.

203 See the ALRC's proposals in this regard: Proposals 4–1, 4–2, 4–3, 4–4, 4–5, 4–6.

44.110 The ALRC is also concerned that a requirement to self-audit may only improve levels of compliance if results are reported and the OPC has the time and resources to monitor self-audit reports produced and conduct spot audits to verify the self-auditing process. This would place a large compliance burden on agencies and organisations, and require significant use of OPC resources. It would also be particularly onerous for small businesses, if the ALRC's proposal to abolish the small business exemption were implemented.[204]

44.111 For these reasons, the ALRC's preliminary view is that agencies and organisations should not be required to self-audit and report on privacy compliance. The OPC should continue, however, to educate agencies and organisations on the value of self-auditing, including to ensure compliance with the proposed 'Openness' principle.[205] The OPC should also clarify situations where it will regard a self-audit policy as a reasonable step to take to ensure the protection of personal information held, in compliance with the proposed 'Data Security' principle.[206]

Functions under other Acts

Background

44.112 In addition to the functions enumerated in the *Privacy Act*, the Commissioner has functions under other legislation.[207] In summary, these functions are to:

- Issue the *Data-matching Program (Assistance and Tax) Guidelines* and to investigate an act or practice that may breach the Guidelines or Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth).[208]

- Issue the *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines* and to investigate an act or practice that may breach the guidelines.[209]

- Monitor compliance with the record keeping requirements under Part 13 of the *Telecommunications Act 1997* (Cth).[210] The Commissioner must also be consulted about industry codes and standards that deal with privacy issues

---

204 See Proposal 35–1.

205 In particular, self-auditing can help agencies and organisations ensure that they have an adequate Privacy Policy in place. See also Ch 21. A similar suggestion was made in Veda Advantage, *Submission PR 163,* 31 January 2007.

206 See Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

207 These functions are set out in more detail in Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [6.66]–[6.75].

208 Issued pursuant to *Privacy Act 1988* (Cth) s 27(1)(p) and *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 12(2). These replaced the interim guidelines set out in *Privacy Act 1988* (Cth) sch 2. The current guidelines came into effect on 14 April 1997.

209 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997), 2–3.

210 *Telecommunications Act 1997* (Cth) s 309.

pursuant to Part 6 of the *Telecommunications Act*[211] and must be consulted before the Australian Communications and Media Authority (ACMA) enforces an industry code relating to a matter dealt with by the NPPs or an approved privacy code.[212]

- Investigate and determine complaints about breaches of the spent convictions scheme in Part VIIC of the *Crimes Act* and to assess applications for complete or partial exclusions from the requirements of the scheme.[213]

Submissions and consultations

44.113 In IP 31, the ALRC asked whether all the Commissioner's functions be consolidated in the *Privacy Act*.[214] All stakeholders who commented on this issue were supportive of consolidation.[215] For example, the OPC noted that, consistent with its argument that the *Privacy Act* be restructured to take a more logical format to assist the ease of use for the reader, it supported the consolidation of the Commissioner's functions into one section of the Act, including where the functions are presently under other legislation.[216]

ALRC's view

44.114 Consistently with the ALRC's proposal that the *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity,[217] the ALRC believes it would add transparency to the role of the OPC to list all of the OPC's functions in the *Privacy Act*, including those under other legislation. Ideally, this would be achieved by amending the *Privacy Act* to list all of the Commissioner's functions as they currently stand, and ensuring that any new legislation that confers powers and functions on the Commissioner also consequentially amends the list.[218]

---

211 Ibid ss 117(1)(j), 117(1)(k), 118, 134. In 2005–06, the Privacy Commissioner was consulted on 12 Australian Communications Industry Forum codes developed pursuant to the *Telecommunications Act 1997* (Cth): Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), [1.6.1].

212 *Telecommunications Act 1997* (Cth) ss 121, 122.

213 *Crimes Act 1914* (Cth) ss 85ZZ, 85ZZC.

214 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–11.

215 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007. It was also suggested that the Commissioner's functions be listed in a separate schedule to the Act: Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

216 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

217 See Proposal 3–2.

218 An example of such a provision can be found in the *Australian Securities and Investments Commission Act*, which sets out a list of Acts which confer functions and powers on ASIC (in addition to the functions set out in the ASIC Act itself): *Australian Securities and Investments Commission Act 2001* (Cth) s 12A(1).

44.115 The ALRC recognises, however, that with the pace of change in developing and amending legislation, it may not be feasible to expect these consequential amendments to be made. A practical solution may be for the OPC to maintain a list of all the Commissioner's functions in a clearly marked place on its website, and update that list where a new function is conferred or an existing one is changed or removed. The ALRC notes that the OPC already maintains a list of 'Related Legislation' under which the Commissioner has responsibilities.[219] This list could be enhanced by specifying in more detail the functions vested in the Commissioner under the respective Acts, including references to the relevant sections, and in all cases including a hyperlink to the legislation.[220]

Proposal 44–7 The Office of the Privacy Commissioner should maintain and publish on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.

Public interest determinations

Background

44.116 The Commissioner has the power to make a determination that an act or practice of an agency or organisation, which may otherwise breach an IPP, NPP or approved privacy code, should be regarded as not breaching that principle or privacy code while the determination is in force. Such a determination is called a 'public interest determination' (PID) and is issued under Part VI of the *Privacy Act*.[221]

Nature of determinations

44.117 A PID can be made if the public interest in an agency or organisation doing an act or engaging in a practice which breaches or may breach an applicable IPP, NPP or code provision outweighs *to a substantial degree* the public interest in adhering to the IPP, NPP, or code provision.[222] A PID made by the Commissioner in relation to

---

219 See Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 30 July 2007.

220 This is consistent with the approach taken on the Federal Court of Australia website, which lists all Acts that confer jurisdiction on the Federal Court, with hyperlinks to the full text of the consolidated Act: Federal Court of Australia, *Acts which Confer Jurisdiction (as at 30 June 2006)* <www.fedcourt.gov.au/aboutct/aboutct_jurisdiction_acts.html> at 31 July 2007.

221 There are similar instruments in other Australian jurisdictions: see *Information Act 2002* (NT) s 81; *Privacy and Personal Information Protection Act 1998* (NSW) s 41. As at 1 July 2007, there were nine public interest determinations registered, dated from September 1989 with the most recent determination dated October 2002. There are no current temporary public interest determinations: Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 31 July 2007.

222 *Privacy Act 1988* (Cth) s 72(1)–(2). Emphasis added.

organisations (but not agencies) can be given general effect so that it covers all organisations in respect of that act or practice.[223]

44.118 The *Privacy Act* sets out a detailed process for receiving and application for, consulting on, and issuing a PID. The OPC has issued non-binding guidelines to assist those considering or making applications for a PID,[224] and 'strongly encourages' agencies and organisations to discuss matters with the OPC before making an application.[225]

Temporary public interest determinations

44.119 The Commissioner also has the power to issue a temporary public interest determination (TPID). A TPID has the same effect as a PID but is limited in duration to a maximum of 12 months.[226] The Commissioner can make a TPID in relation to an act or practice of an agency or organisation that is the subject of an application for a standard PID where the application raises issues that require an urgent decision.[227] The Commissioner can give a TPID in respect of an act or practice of an organisation general effect, so that it applies to other organisations.[228]

Submissions and consultations

44.120 In IP 31, the ALRC asked whether the Commissioner's powers to make PIDs and TPIDs were appropriate and administered effectively.[229] Most stakeholders submitted that the powers are appropriate,[230] with the OPC suggesting that they provided 'necessary flexibility' to respond to situations where 'the operation of the high level privacy principles in the *Privacy Act* may be inconsistent with the public interest'.[231]

44.121 The Australian Privacy Foundation found that the powers to make PIDs are generally appropriate but have not been used often.[232] Other stakeholders noted

---

223 Ibid s 72(4).

224 Office of the Federal Privacy Commissioner, *Public Interest Determination Procedure Guidelines* (2002).

225 See the Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 31 July 2007.

226 *Privacy Act 1988* (Cth) ss 80A(3)(a), 80B.

227 Ibid s 80A(1).

228 Ibid s 80B(3)–(4).

229 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–18.

230 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

231 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. Similar comments on the benefits of PIDs were made in Australian Federal Police, *Submission PR 186,* 9 February 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

232 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. The limited use of PIDs was also noted in Australian Federal Police, *Submission PR 186,* 9 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

problems with the process of getting a PID. The Office of the Information Commissioner Northern Territory considered that the OPC should be given 'greater flexibility in the process to be adopted prior to a determination' and that Part VI could be simplified significantly.[233] The Insolvency and Trustee Service Australia stated that the PID process 'appears to be cumbersome and there does not appear to be much guidance'.[234] The Australian Privacy Foundation also noted the significant consultation and delay involved in getting a PID, but concluded that this was 'appropriate given that they have the effect of weakening the level of privacy protection'.[235] It suggested, however, that the Commissioner needs 'to be mindful of the burden which detailed PID consultations place on unfunded consumer organisations'.[236]

44.122 The OPC noted that it lacks any discretion under the Act to dismiss an application for a PID or decline to consider it. This means that once an application is made to the OPC, it must embark on the lengthy consultation process set out in the Act. The OPC submitted that 'as such, there is a risk that an application could be made frivolously or vexatiously or where there is clearly no merit and the Commissioner would then be bound to undertake full consideration of the matter'. The OPC recommended that the Act be amended to require an applicant to consult with the OPC before making an application or give the Commissioner a discretion not to consider an application if it is clearly of no merit. The OPC noted that either decision would be subject to judicial review.[237]

ALRC's view

44.123 The ALRC does not propose any reform to the public interest test for the making of a PID or TPID at this stage. The ALRC is, however, proposing reform to the parallel test used in relation to medical research. Under those provisions, where research may breach the IPPs or NPPs, the medical research guidelines provide that the research must be approved by a HREC.[238] Before approving a particular research proposal under the guidelines, HRECs are required to consider whether the public interest in the research substantially outweighs the public interest in the protection of privacy. In Chapter 58, the ALRC proposes that this test should be changed to whether the public interest in the research *outweighs* the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs.

44.124 The ALRC does not propose that a similar change be made to the PID test. There are significant differences between a PID and the approval of a research proposal by an HREC. PIDs have the potential to reduce the protection provided by the

---

233 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
234 Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007.
235 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
236 Ibid.
237 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
238 The medical research guidelines are issued by the National Health and Medical Research Committee and approved by the Privacy Commissioner under ss 95 and 95A of the *Privacy Act 1988* (Cth). Ch 58 discusses these guidelines in more detail.

privacy principles across broad sectors for significant periods of time. In contrast, approval by an HREC is limited to specific research activities for the duration of those activities.

44.125 In relation to the process involved in issuing a PID, the ALRC acknowledges that the *Privacy Act* provisions are more prescriptive than their counterparts in the states and territories. The ALRC recognises that it is a resource-intensive process to undertake where an application clearly has little or no merit, or is frivolous, vexatious or misconceived—for both the OPC and for consumer and privacy groups that contribute to the consultation process. Accordingly, the ALRC's view is that the *Privacy Act* should be amended to give the Commissioner discretion to decline to accept an application for a PID where the Commissioner is satisfied that the application is frivolous, vexatious, misconceived or lacking in merit. This proposal would set a high standard for dismissing an application outright, and should operate to encourage applicants to discuss their applications with the Commissioner before submitting them, consistent with the PID guidelines. The ALRC also notes that any decision to refuse to accept an application would be subject to judicial review.

Proposal 44–8 The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a public interest determination where the Privacy Commissioner is satisfied that the application is frivolous, vexatious, misconceived or lacking in merit.

Privacy codes

Background

44.126 When bringing organisations within the ambit of the *Privacy Act*, Parliament decided to adopt a co-regulatory approach. It established a framework in which organisations are able to develop specialised codes for the handling of personal information which, when approved, replace the NPPs.[239] This approach was 'designed to allow for flexibility in an organisation's approach to privacy, but at the same time, guarantees consumers that their personal information is subject to minimum standards that are enforceable in law'.[240]

Commissioner's powers in relation to codes

44.127 Part IIIAA of the *Privacy Act* sets out provisions on privacy codes. The Commissioner's powers regarding privacy codes are generally to:

239 Ibid s 16A. The code may also cover exempt acts or practices: s 18BAA.

240 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001), 16. See also the comments made in the Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 19.

- approve privacy codes and variations of approved privacy codes and to revoke those approvals;[241]

- review the operation of approved privacy codes;[242]

- prepare and publish guidelines about development, approval and variation of privacy codes, and about complaint handling processes under codes;[243]

- perform functions and exercise powers conferred on an adjudicator under an approved privacy code where the Commissioner has been appointed as the independent adjudicator under that code;[244] and

- consider applications for review of determinations of adjudicators (other than where the Commissioner is the adjudicator) in relation to a complaint.[245]

Requirements for codes

44.128 The content of a code must meet set standards. In particular, a code must incorporate all the NPPs or set out 'obligations that, overall, are at least the equivalent of all the obligations set out in those Principles'.[246] Subscription to a code is voluntary. Codes must specify the organisations to which they apply, and may be approved even where they apply for a limited period or to a specified activity or industry sector.[247] If the code sets out procedures for making and dealing with complaints, these processes must comply with the Commissioner's guidelines and the prescribed standards.[248]

44.129 Codes are legislative instruments under s 5 of the *Legislative Instruments Act 2003* (Cth). A privacy code approved under Part IIIAA is not, however, subject to disallowance by Parliament.[249] There are currently three codes listed on the Register of Approved Privacy Codes found on the OPC's website and two code applications currently being considered by the OPC.[250]

---

241 *Privacy Act 1988* (Cth) s 27(1)(aa).
242 Ibid s 27(1)(ad). Review occurs under s 18BH.
243 Ibid s 27(1)(ea).
244 Ibid s 27(1)(ac).
245 Ibid s 27(1)(ae). See also s 18BI.
246 Ibid s 18BB(2)(a).
247 Ibid ss 18BB(2)(b)–(c), (6)–(7).
248 Ibid s 18BB(3)(a).
249 *Legislative Instruments Act 2003* (Cth) s 44(2), item 44; *Legislative Instruments Regulations 2004* (Cth) sch 2, cl 8. Note that an approval of a variation of a privacy code and a revocation of an approval of an approved privacy code, or revocation of a variation of an approved privacy code are also nominated as legislative instruments that are not subject to disallowance: cls 8A, 8B.
250 Codes currently in operation are the Market and Social Research Privacy Code, administered by the Association of Market Research Organisations; the Queensland Club Industry Privacy Code, administered by Clubs Queensland; and the Biometrics Institute Privacy Code, administered by the Biometrics Institute. There was a fourth code approved by the Privacy Commissioner (the General Insurance Information Privacy Code), revoked on 30 April 2006. Code applications currently being considered by the OPC are the Australian Casino Association Privacy Code and the Internet Industry

Code development process

44.130 Before the Commissioner can approve a code, he or she must be satisfied that members of the public have been given an adequate opportunity to comment on a draft of the code.[251] This requirement for public consultation is just one part of the process involved in developing a code. The Guidelines on Privacy Code Development (Code Guidelines) issued by the OPC in 2001 set out the detailed process involved in making a privacy code, including requirements in relation to NPP equivalence, explanatory material, coverage, voluntary membership, code review and drafting standards. In deciding whether to approve a privacy code, the Commissioner may consider the matters specified in the Code Guidelines.[252] Following various comments from stakeholders about the complex and costly code approval process, the OPC Review recommended that the Office review the Code Guidelines with a view to simplifying them.[253]

Binding Codes

44.131 The Commissioner cannot initiate a privacy code and cannot make it binding on organisations that do not consent to be bound by the code. The issue of binding codes was discussed in detail in the OPC Review and the Senate Committee privacy inquiry. In the former, stakeholders submitted that the Commissioner should have power to formulate and impose binding codes even where an organisation does not consent to being subject to a code. It was argued that this would be one way of solving systemic issues in privacy compliance.[254] Although support for this proposition was not universal, the OPC recommended that the Australian Government consider amending the *Privacy Act* to give the Commissioner power to make binding codes and suggested a number of models for the power, as discussed below.[255]

44.132 The Senate Committee privacy inquiry also considered binding codes, and noted the explanation given by the Privacy Commissioner on the difference between privacy codes approved under Part IIIAA and the OPC Review's proposal for binding codes:

> The idea of the binding codes that we have suggested is to come up in other areas where perhaps they were not going to be voluntary. The NPP codes are developed on

---

Privacy Code. See Office of the Privacy Commissioner, *Privacy Codes* <www.privacy.gov.au/business> at 31 July 2007.

251 *Privacy Act 1988* (Cth) s 18BB(2)(f).

252 Ibid s 18BB(4).

253 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 47. See discussion about codes at 166–171.

254 Ibid, 145.

255 Ibid, recs 7 and 44. See related recommendations in recs 16 and 73. For discussion about models, see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46–47.

> a voluntary basis. The ones that were binding could possibly be done for technology, or for an industry that was not working as well—perhaps the tenancy database area.[256]

44.133 The New Zealand Privacy Commissioner has the power to issue binding codes of practice that become part of the law.[257] The Codes may modify the application of one or more of the information privacy principles by prescribing standards that are more stringent or less stringent than the standards prescribed by the principle, or by prescribing how any one or more of the principles are to be applied, or are to be complied with.[258] The Codes may modify the operation of the Act for specific industries, agencies, activities or types of personal information.[259] Proposals for issuing a code can be made by a body representing the interests of a particular class of agency or industry or by the Privacy Commissioner.[260]

Prescribed industry codes under the Trade Practices Act

44.134 One of the models put forward by the OPC for a binding code power was Part IVB of the *Trade Practices Act 1974* (Cth) (TPA). Under the TPA, the Minister has the power to prescribe an industry code of conduct in the regulations.[261] The regulations declare the industry code to be a mandatory industry code or a voluntary industry code. A prescribed mandatory code of conduct is binding on all industry participants.[262] The Act makes the codes enforceable by prohibiting a corporation, in trade or commerce, from contravening an applicable industry code.[263]

44.135 At a practical level, formal proposals for TPA codes are initiated at the ministerial level, 'following representations from industry participants, consumers or government authorities about problems in a particular industry'.[264] As the regulator under the TPA, the ACCC is responsible for promoting compliance with codes by providing education and information and, where necessary, by taking enforcement action. Since introducing these provisions in 1998, three mandatory codes of conduct have been prescribed under the TPA.[265]

---

256 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 97–98.

257 *Privacy Act 1993* (NZ) pt 6. Note the Privacy Commissioner in NSW has similar powers to initiate binding privacy codes: *Privacy and Personal Information Protection Act 1998* (NSW) pt 3, div 1.

258 *Privacy Act 1993* (NZ) s 46(2).

259 Ibid s 46(3).

260 Ibid s 47.

261 *Trade Practices Act 1974* (Cth) pt IVB.

262 Ibid s 51AE.

263 Ibid s 51AD.

264 J Hockey, *Prescribed Codes of Conduct: Policy Guidelines on Making Industry Codes of Conduct Enforceable under the Trade Practices Act 1974* (1999) Australian Government Treasury, 6.

265 See *Trade Practices (Industry Codes – Franchising) Regulations 1998* (Cth); *Trade Practices (Industry Codes – Oilcode) Regulations 2006* (Cth); *Trade Practices (Horticultural Code of Conduct) Regulations 2006* (Cth).

Industry codes and standards in the Telecommunications Act

44.136 Another model put forward by the OPC was Part 6 of the *Telecommunications Act 1997* (Cth). Under this Act, bodies and associations that represent sections of certain industries may develop industry codes, which may be registered by ACMA. Compliance with the code is voluntary unless otherwise directed by ACMA.[266] In addition, ACMA can request a body or association to develop an industry code.[267] If the request is refused or the code prepared following a request is not registered by ACMA, or if an existing code is deficient, ACMA may determine an 'industry standard'.[268]

44.137 In making an industry standard, ACMA must be satisfied that it is necessary or convenient for it to determine a standard in order to provide appropriate community safeguards in relation to the matter, or otherwise regulate adequately participants in that section of the industry.[269] Compliance with an industry standard is mandatory; each participant in the section of an industry to which the standard applies must comply with the standard.[270] Breach of the standard is subject to a civil penalty and ACMA may issue a formal warning if a person contravenes an industry standard registered under Part 6.[271] An industry standard is a disallowable instrument and the Act specifies that ACMA must undertake public consultation on industry standards, and must also consult with consumer bodies and relevant regulators.[272]

Binding guidelines

44.138 A potential subset of binding codes, or an alternative to them, is the concept of binding guidelines. The benefits of giving the Commissioner a general power to issue binding guidelines was discussed in the OPC Review. It was suggested that such a power 'could be a useful tool in contexts where the Office becomes aware of systemic issues and wishes to issue general, but binding guidance to ensure that all organisations comply with them'.[273] The guidelines

> could address aspects of the NPPs as they are applied in specific contexts, for example, steps to be taken in a particular industry sector to ensure personal information is accurate, complete and up to date. They could overcome uncertainty in application of NPPs in particular situations. It would also benefit consumers to have a more specific idea of their rights.[274]

---

266 *Telecommunications Act 1997* (Cth) s 121.
267 Ibid s 118.
268 Ibid ss 123, 125.
269 Ibid s 123(1)(c).
270 Ibid s 128.
271 Ibid s 129.
272 Ibid s 133–135A.
273 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 158.
274 Ibid, 158.

Submissions and consultations

44.139 The ALRC asked a series of questions in IP 31 about privacy codes, including whether the provisions for approving privacy codes are appropriate and effective, whether privacy codes are an appropriate method of regulating and complying with the Act, why have they been so little used, and whether the Commissioner should have the power, on his or her initiative, to develop and impose a binding code on agencies or organisations.[275] The ALRC also asked for views on whether the Commissioner should have power to issue binding guidelines, and if so, in what circumstances.[276]

Existing code provisions

44.140 The OPC reiterated its conclusion from the OPC Review that, 'given the lack of take up in codes and the revocation of the only code that established its own complaint handling process, it is reasonable to conclude that the code making provisions have not been highly successful in their current form'.[277] The OPC raised several issues with codes, one being that there is tension between the concept of national consistency and industry privacy codes, in that a proliferation in industry codes may increase the complexity and fragmentation of privacy regulation for individuals, organisations and agencies. The OPC also noted that it had not derived any significant efficiency benefits from codes, as the Commissioner remains the complaint-handling body. This in turn raises the risk that the OPC's compliance role will become increasingly complex and cumbersome, as complaint staff will have to apply different sets of principles for different complaints.

44.141 The OPC also noted that despite its recommendation that the Code Guidelines be simplified, the code approval process is likely to continue to be 'lengthy and potentially complicated' given that it must assess whether the code provisions offer an equivalent protection to the NPPs. The OPC did not, however, support the removal of the equivalence requirement or a model under which codes would be able to derogate from, or waive compliance with, the principles. It nominated the PID mechanism as the more appropriate process to deal with applications to waive NPPs in certain circumstances.[278]

44.142 Given these concerns, the OPC suggested that 'there is strong argument to amend the code provisions in the interests of efficiency and national consistency'. The OPC proposed two ways to achieve this. The first was to give the Commissioner discretion to decline to consider a proposal for a code where there is little or no public interest in code development. Public interest in this situation would involve weighing up the need for a code against the impact on national consistency and the costs involved. Secondly, codes could operate in addition to the privacy principles rather than replacing the principles, similarly to the *Credit Reporting Code of Conduct*. This

---

275 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–20.
276 See Ibid, [6.57].
277 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
278 Ibid.

would mean that privacy principles would apply as a base standard across the community (supporting national consistency) and the code would then provide specific and binding guidelines on how the NPPs should be applied in particular sectors. The OPC gave the example of a real estate industry code that could specify the types of information that could be considered, under NPP 1.1, as 'necessary' to collect in a tenancy application process.[279]

44.143 The NHMRC also considered the tension between codes and national consistency. It expressed concern that the 'current provisions for voluntary codes add (unhelpfully) to the complexity of the federal privacy regulatory regime'.[280] The NHMRC was particularly concerned about codes that apply horizontally rather than vertically.

> If organisations delivering health care and conducting health and medical research subscribed to such a code, they would be required to comply with additional and/or different regulatory requirements covering only a proportion of their activities. We consider that this creates a significant disincentive for such organisations to subscribe to voluntary codes that apply horizontally.[281]

44.144 Other stakeholders commented more generally on the Commissioner's code-making powers. The Australian Privacy Foundation noted that while the code-making provisions are 'potentially useful', it is not surprising they have been so little used as code making involves a significant commitment of resource from a code's proponent with little benefit.[282] The Foundation submitted that it would helpful to extend the code provisions to apply to agencies and noted that this would allow the Biometrics Code to be enforced against any agencies that adopted it.[283] The Foundation also submitted that codes could prove useful in interpreting the application of privacy principles in the context of specific sectors or technologies.[284] As applications from organisations would be unlikely, the Australian Privacy Foundation considered that the Commissioner should have the power to initiate code development.[285]

44.145 Several other stakeholders supported a continuation of the co-regulatory approach.[286] For example, DEWR supported the maintenance of a non-prescriptive approach to privacy regulation, noting that the 'ability for organisations and industry sectors to develop their own privacy codes is a key element of the flexibility inherent

---

279 Ibid.
280 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
281 Ibid.
282 The onerous costs of code development were also noted in other submissions: eg, Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
283 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
284 See also Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007.
285 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
286 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

in the current *Privacy Act'*.[287] Similarly, the Centre for Law and Genetics supported the continuation of a co-regulatory model, but submitted that the process for developing, approving and implementing privacy codes must be improved. The Centre also suggested that the OPC must be given greater authority to ensure that the code side of the co-regulatory model works, with strengthened enforcement provisions.[288]

Binding codes and guidelines

44.146 In relation to binding codes and binding guidelines, the OPC reiterated its recommendation from the OPC Review that it 'be provided with the power to make binding codes as a component of a more robust compliance regime that is responsive to arising privacy issues'.[289] It submitted that the code-making power could be based on the 'prescribed industry code' model in Part IV of the TPA or the 'prescribed standard' model in Part 6 of the *Telecommunications Act*, and it would:

> - Provide the Commissioner with an effective and efficient means of responding to recurrent privacy issues within a particular sector and thereby create a more level playing field among organisations, and ensuring that conscientious organisations are not commercially disadvantaged
> - Provide an opportunity to give clear guidance for individuals and organisations regarding how the *Privacy Act* applies in particular circumstances
> - Provide the *Privacy Act* with sufficient flexibility to respond to new and emerging privacy issues, including those that relate to technologies …[290]

44.147 The OPC emphasised in its submission that 'any power to issue binding guidelines or codes should necessitate significant consultation with affected stakeholders' and that as a further accountability mechanism, binding codes initiated by the Commissioner should be disallowable instruments.[291]

44.148 The Office of the NSW Privacy Commission supported providing the Commissioner with the power to develop binding statutory codes and/or guidelines in cases where there is a strong public interest or it is clear that systemic issues need to be addressed. It suggested that codes would become part of the uniform set of privacy principles and:

> would be especially useful in addressing privacy issues/problems in an organisation/industry-specific context, creating less uncertainty about the application of privacy principles in that context, as well as clarifying the scope of protection with prescriptive requirements.[292]

---

287 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.
288 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
289 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
290 Ibid.
291 Ibid.
292 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

44.149 The Centre for Law and Genetics submitted that the OPC 'must have power, where there has been a failure by the industry after reasonable notice, to develop and impose a binding code'. The Centre described binding codes as 'another crucial issue for the development of our preferred approach of general guidance principles supported by industry codes'.[293] Similarly, Legal Aid Queensland supported the recommendations of the OPC that it have the power to make a binding code, and suggested, along with a number of other stakeholders, that the Commissioner should make a binding code for residential tenancy databases.[294]

44.150 The NHMRC submitted that the incorporation of a binding-code power in the *Privacy Act* would achieve 'only a marginal improvement of the current complex and confusing regime'.[295] Given its concerns about codes not being taken up uniformly across a sector, the NHMRC nevertheless expressed 'in principle' support for giving the Commissioner power to formulate and impose binding codes, on the basis that 'uniform imposition of a code within the sector which is subject to the *Privacy Act* would be preferable to its partial voluntary uptake'.[296] It specified that a binding code must be developed through a collaborative and consultative process and must replace rather than complement existing regulation. It also submitted that the code must apply to entire industry sectors and organisations rather than specific technologies or functions.

44.151 DEWR did not support the OPC having a statutory power to develop and impose privacy codes on the private sector, stating that a 'combination of market forces and advice and directed advocacy from the OPC and other government bodies with an interest in information privacy is sufficient for organisations to adopt appropriate information privacy principles and practices'. It also noted the risk that 'externally-imposed codes and practices will not be adhered to if they involve significant costs to those subject to them'.[297]

ALRC's view

Reforming the current code provisions

44.152 One of the consistent themes discussed by stakeholders in this Inquiry involves the need to promote national consistency and to reduce fragmentation, complexity and confusion in privacy regulation. In support of this goal, the ALRC believes that codes should operate in addition to the privacy principles, rather than

---

293 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

294 Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

295 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

296 Ibid.

297 Australian Government Department of Employment and Workplace Relations, *Submission PR 211,* 27 February 2007.

replacing them. At all times and for all agencies and organisations subject to the *Privacy Act*, the privacy principles should operate as the base standard. Codes could be used to provide more guidance (however named) on how one or more of the proposed UPPs are to be applied or are to be complied with by the organisation bound by the code. This would resemble the operation of codes in New Zealand.[298]

44.153 Under this model, the guidelines contained in the code must impose obligations equivalent to those imposed by the relevant privacy principle. This relationship between the principle and the guideline in the code can be illustrated as follows. A real estate industry code could prescribe an exhaustive list of information that can be considered 'necessary', under the proposed 'Collection' principle, to collect in a tenancy application process.[299] By specifying particular types of information as those necessary to collect in a tenancy application form, the guidelines would contain equivalent obligations to the principle, as both require that only information that is necessary be collected. The code, however, provides more detailed guidance than the principle and would assist real estate agencies in meeting the outcome set by the principle.

Binding code-making power

44.154 This ability to prescribe standards for one or more of the proposed UPPs would also be a useful regulatory tool for the Commissioner in industries with low levels of compliance and high levels of complaint, or where there are calls for more assistance and consistency in applying privacy principles across the industry. The residential tenancy database industry is a good example, as there continues to be high levels of complaints about operators and the OPC has acknowledged that 'in practice, the impact of the Commissioner's determinations on the tenancy industry appears to have been limited'.[300] The OPC Review also noted that a number of database operators have called for the Commissioner to 'rule' on a number of aspects of the NPPs; the interest seems to be in 'seeking certainty and to some extent a level playing field'.[301]

44.155 The ALRC's view is that the OPC should have a power, first, to request the development of a code and, secondly, to develop and impose a code on its own initiative. The ALRC's preliminary view is that the *Telecommunications Act 1997* (Cth) provides the best model for a binding code power in the privacy context. This model leaves the Commissioner with responsibility for code administration and development rather than the Minister, and can be integrated into the current Part IIIAA provisions.

44.156 Under this model, there could be a three-step process. As a first step, industries would be encouraged, where the OPC or the industry association considered

---

298 See *Privacy Act 1993* (NZ) s 46(2)(b).
299 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
300 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.
301 Ibid, 159.

it appropriate, to develop privacy codes (being the current Part IIIAA codes as amended by the ALRC's proposal). These codes would set standards to bring participants within compliance with the privacy principles. They would operate in addition to the privacy principles, rather than replacing them, and could apply vertically across an industry as well as horizontally. As a second step, the OPC could request an industry to develop an industry code. This power could be exercised in circumstances where the OPC considers that the development of a code is necessary or convenient in order to provide appropriate community safeguards, or deal with inadequate levels of compliance by participants in the industry. It could also be exercised where the OPC does not believe that, in the absence of a request, a code would be developed within a reasonable time. If the industry does not develop a code in response to the request, or the developed code is determined to be inadequate, or a code already in place is deficient, then the OPC could take the third step of prescribing a binding code for the industry. The code would be prescribed only after public consultation and would be a disallowable instrument.

44.157 This model expands the ability of codes to deal with new and developing technologies, by giving the Commissioner power to translate the steps an agency or organisation must take to comply with the proposed UPPs in the context of a particular technology.[302]

44.158 The ALRC notes that codes (whether initiated by industry or the Commissioner) could be used to incorporate the concept of 'no disadvantage' where necessary.[303] As explained in Chapter 29, such a concept promotes the idea that an individual should not be disadvantaged by asserting his or her privacy rights. A code could formalise and clarify existing protections in the privacy principles, such as the requirement in the proposed 'Access and Correction' principle that, if an organisation charges for providing access to personal information, those charges must not be excessive. A code could provide guidance on how to apply this principle to prevent excessive fees, by explaining how to set an access fee and providing examples of reasonable and excessive fees.

Codes versus regulations

44.159 The proposed reforms to the code provisions are to be distinguished from the ALRC's proposals to make regulations for credit reporting and health.[304] The most significant difference between the two instruments is that, if the ALRC's proposed changes are implemented, the privacy principles would always operate as the base standard in a privacy code—the code cannot replace the principles. In contrast, the proposed privacy regulations must be consistent with the objects of the Act but can

---

302 The use of codes to address technological issues is discussed further in Part B.

303 Stakeholders that supported the addition of a no disadvantage principle included: G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

304 See Proposals 50–2 (proposing regulations for credit reporting), and 56–2 (proposing regulations for health information).

modify the operation of the UPPs to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.[305]

44.160 The proposed privacy codes are a form of co-regulation that 'fills in the gaps' between the outcome set by a privacy principle and the application of, or compliance with, that principle. In contrast, the regulations provide flexibility in certain industries, such as credit reporting and health, to provide more or less stringent requirements than those in the principles themselves to achieve better regulatory outcomes.

Proposal 44–9 Part IIIAA of the *Privacy Act* should be amended to specify that:

(a) privacy codes approved under Part IIIAA operate in addition to the proposed UPPs and do not replace those principles; and

(b) a privacy code may provide guidance or standards on how any one or more of the proposed UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that are at least equivalent to those under the Act.

Proposal 44–10 Part IIIAA of the *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) request the development of a privacy code to be approved by the Privacy Commissioner pursuant to s 18BB; and

(b) develop and impose a privacy code that applies to designated agencies and organisations.

305 Proposal 3–1.

45. Investigation and Resolution of Privacy Complaints

Contents

Introduction 1239
Investigating privacy complaints 1240
- Background 1240
- Matters the Commissioner must not investigate 1240
- Discretion not to investigate or to defer investigation 1240
- Submissions and consultations 1241
- ALRC's view 1242

Transferring complaints to other bodies 1244
- Background 1244
- Submissions and consultations 1245
- ALRC's view 1245

Resolution of privacy complaints 1248
- Model under the *Privacy Act* 1248
- Conciliation 1248
- Determinations 1249
- Submissions and consultations 1251
- ALRC's views 1254

Accountability and transparency 1259
- Background 1259
- Merits review 1259
- Complaint-handling policies and procedures 1261

Other issues in the complaint-handling process 1264
- Background 1264
- Representative complaints 1264
- Preliminary inquiries 1266
- Ceasing investigations if certain offences have been committed 1267
- Conduct of investigations 1268

Introduction

45.1 The *Privacy Act 1988* (Cth) provides an avenue for individuals to complain about acts or practices of an agency or organisation that may be an interference with their privacy. The Act vests power in the Privacy Commissioner (Commissioner) to investigate, conciliate and make determinations to finalise complaints.

45.2 This chapter considers issues concerning the investigation and resolution of complaints under the *Privacy Act*. The chapter examines concerns about accountability and transparency in the Act and in the policies and procedures of the Office of the Privacy Commissioner (OPC) with regard to complaint handling. The chapter also considers some particular issues raised by stakeholders in relation to representative complaints, preliminary inquiries, and the conduct of investigations.

Investigating privacy complaints

Background

45.3 The Commissioner's powers to investigate complaints of a breach of the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) are established in separate paragraphs of s 27(1).[1] The trigger that enlivens these powers is that a 'complaint' is made. The *Privacy Act* confers rights on individuals to complain to the Commissioner about acts or practices that may be an interference with individuals' privacy rights, as created by the *Privacy Act*.[2]

Matters the Commissioner must not investigate

45.4 The Commissioner is generally required to investigate an act or practice if it may be an interference with an individual's privacy and a complaint has been made about it under s 36.[3] The Commissioner must not investigate a complaint, however, if the complainant did not complain to the respondent before complaining to the Commissioner under s 36, unless the Commissioner considers that it was not appropriate for the complainant to complain to the respondent.[4] The Commissioner must also cease investigating if certain offences have been committed, or where the Auditor General is already investigating the matter.[5] These last two situations are discussed later in this chapter.

Discretion not to investigate or to defer investigation

45.5 The Commissioner has the discretion to decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under s 36, or accepted under s 40(1B), where the:

---

1 *Privacy Act 1988* (Cth) ss 27(1)(a), 27(1)(ab).

2 Ibid s 36. Note, there is no right to complain to the Commissioner about acts or practices of an organisation bound by an approved privacy code where the code contains a procedure for making and dealing with complaints to an adjudicator, and the code is relevant to the act or practice in question: see s 36(1A).

3 Ibid s 40(1). The power to investigate on the Commissioner's own motion is discussed in Ch 46.

4 Ibid s 40(1A). In practice, the OPC requires that complainants provide it with a copy of their letter to the respondent and a copy of any response received by the complainant. The OPC requires that the complainant give the respondent 30 days to reply to the letter of complaint: see Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

5 *Privacy Act 1988* (Cth) ss 49, 51.

- act or practice is not an interference with privacy; the complaint was made over 12 months after the complainant became aware of the act or practice; the complaint is frivolous, vexatious, misconceived or lacking in substance; the act or practice is the subject of an application under another federal, state or territory law and the complaint is being dealt with adequately under that law; or another law provides a more appropriate remedy for the complaint;[6]

- complainant has complained to the respondent about the act or practice and the respondent is dealing adequately with the complaint or has not yet had an adequate opportunity to deal with the complaint;[7] or

- respondent has applied for a public interest determination and the Commissioner is satisfied that the interests of persons affected by the act or practice would not be unreasonably prejudiced if the investigation were deferred until the application has been disposed of.[8]

Submissions and consultations

45.6 Stakeholders commented on the requirement that a complainant must complain to the respondent before making a complaint to the Commissioner. For example, the Consumer Credit Legal Centre (NSW) (CCLC) submitted that the requirement is 'overly bureaucratic' and must be reconsidered, particularly in the credit reporting context, where

> a complaint may be required to be made in writing up to four times before it can be addressed as it could involve both the credit reporting agency and the credit provider as respondents. This delays the process and the complainant is prejudiced by the delay as a disputed default listing prevents them from getting credit. This obviously is not an effective complaint mechanism.[9]

45.7 In contrast, the OPC strongly supported the retention of a 'general requirement that individuals complain to the body with whom they have the grievance in the first instance'.[10] The OPC suggested the requirement was consistent with those of other regulators and provides respondents 'with an opportunity to take greater control and ownership of their handling of complaints', and an incentive to deal actively with matters before they are raised with the Commissioner.[11]

---

6 See Ibid s 41(1).
7 Ibid s 41(2).
8 Ibid s 41(3).
9 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 139. The discussion of the complaint 'merry-go-round' in the credit reporting context is addressed in Ch 55.
10 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
11 Ibid.

45.8 The OPC and the Commonwealth Ombudsman commented on the Commissioner's discretions under the *Privacy Act* not to investigate a complaint, or not to investigate it further. The OPC considered its discretions in the context of trying to find a balance between focusing on individual complaints and addressing broader systemic issues. To achieve this balance, the OPC recommended that the Commissioner be granted a discretionary power to decline to investigate complaints where there appears to be little public interest, such as where there is minimal apparent harm or the matter has been considered before and the organisation has changed its practices.[12] The OPC suggested that the proposed power could be balanced by a requirement that the OPC advise the respondent that a complaint has been lodged and, while it is not being investigated, any further complaints of a similar nature may be. The OPC pointed to similar powers to decline vested in other complaint handlers, such as the power of the Human Rights and Equal Opportunity Commission (HREOC) to decline to investigate where the complaint is trivial.[13]

45.9 The Commonwealth Ombudsman described the OPC's discretions under s 41 as 'narrower' than the Ombudsman's.[14] The Ombudsman explained that a common basis for declining to investigate a complaint under the *Ombudsman Act 1976* (Cth) is that an investigation would not be warranted in all the circumstances.[15] This power enables it 'to decide not to investigate where, for example, the matter is trivial, there is no practical remedy or where there is no prospect of a satisfactory resolution'.[16]

45.10 The OPC also observed that the Commissioner lacks the specific discretion to cease an investigation where a complainant repeatedly fails to respond to correspondence from the OPC. The OPC suggested that it would be preferable for the Commissioner to have a specific power to stop investigating a complaint if the complainant has ceased to pursue the matter or has withdrawn the complaint.[17]

ALRC's view

45.11 A central tension in regulating compliance with the *Privacy Act* is how to strike a balance between resolving individual complaints and remedying systemic issues. By systemic issues, the ALRC is referring to 'issues that are about an organisation's or industry's practice rather than about an isolated incident'.[18] Systemic issues can be distinguished from issues that have no implications beyond the immediate actions and

---

12 The OPC made a similar recommendation in Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 46.

13 See *Human Rights and Equal Opportunity Act 1986* (Cth) s 46PH(1)(c). The NSW Privacy Commissioner also has the discretion to dismiss trivial complaints: see *Privacy and Personal Information Protection Act 1998* (NSW) s 46(3)(b).

14 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.

15 See *Ombudsman Act 1976* (Cth) s 6(1)(b)(iii).

16 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007. The OPC also commented on this power: Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

17 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

18 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 130 fn 102.

rights of the parties to the complaint.[19] They can, however, be identified out of the consideration of a single complaint, 'because the *effect* of the particular issue will clearly extend beyond the parties to the complaint'.[20]

45.12 In the ALRC's view, a compromise needs to be made between addressing individual complaints and addressing systemic issues. The compromise proposed by the ALRC is to give the Commissioner more discretion not to investigate individual complaints in certain circumstances. First, the ALRC proposes that the Commissioner should be given discretion not to investigate an act or practice if he or she is satisfied that an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances. This discretion would enable the Commissioner to dismiss trivial complaints, or complaints that have no prospect of a practical or satisfactory resolution.[21]

45.13 Secondly, the ALRC believes the Commissioner's powers to dismiss stale complaints should be clarified. The ALRC proposes that the *Privacy Act* be amended to give the Commissioner the specific discretion to cease investigating a complaint that has been withdrawn by the complainant; or where the Commissioner has had no substantive response from the complainant for a certain period, following a request by the Commissioner for a response in relation to the complaint.[22]

45.14 The ALRC does not propose any reform to the requirement that complainants first complain to the respondent. The ALRC agrees with the OPC that where a complaint can be resolved between the complainant and respondent without involving the OPC, this is likely to be the most efficient means of resolving it. This approach is also consistent with other privacy legislation and the approach taken in external dispute resolution (EDR) schemes such as the Banking and Financial Service Ombudsman (BFSO) and the Telecommunications Industry Ombudsman (TIO).[23] The obligation on complainants to complain first to the respondent should, however, be supported by agencies and organisations adopting internal dispute resolution processes and making the avenues of complaint clear in their Privacy Policies.[24]

---

19 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999, [PS 139.131]–[PS 139.133].

20 Ibid, [PS 139.131]–[PS 139.133]. A similar definition was put forward in Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

21 Other statutes also have a similar test: *Anti-Discrimination Act 1977* (NSW) s 92(1)(a)(iii).

22 Examples of similar provisions include: *Health Records Act 2001* (Vic) s 53(1); *Information Privacy Act 2000* (Vic) s 30.

23 See, eg, *Information Privacy Act 2000* (Vic) s 29; *Health Records Act 2001* (Vic) s 51; *Ombudsman Act 1976* (Cth) s 6; Banking and Financial Services Ombudsman, *About Us* <www.abio.org.au> at 1 August 2007; *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [5].

24 This is consistent with Proposal 21–2.

Proposal 45–1 Section 41(1) of the *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under s 36, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that:

(a) the complainant has withdrawn the complaint; or

(b) the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or

(c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.

Transferring complaints to other bodies

Background

45.15 The *Privacy Act* contemplates the use of other bodies to resolve privacy complaints. For example, a privacy code approved under the Act can provide procedures for dealing with complaints under the code. The *Privacy Act* also vests the Commissioner with discretion to refer complaints on to other bodies. Where the Commissioner forms the view that the complaint could have been made to HREOC, the Commonwealth Ombudsman, the Postal Industry Ombudsman or the Public Service Commissioner, and would be dealt with more effectively or conveniently by one of those bodies, the Commissioner may decide not to investigate, or further investigate, the matter, and can transfer the complaint to the relevant body.[25]

45.16 Independent of the *Privacy Act* provisions, there are also several EDR schemes that have jurisdiction to deal with privacy complaints under their terms of reference, including the BFSO and TIO.[26]

45.17 The OPC Review considered improving liaison with overlapping complaint handlers, to maximise efficiency and minimise confusion and costs for individuals and organisations.[27] In 2006, the OPC entered into a memorandum of understanding with the Commonwealth Ombudsman, to 'facilitate the exchange of information, subject to

25 *Privacy Act 1988* (Cth) s 50.

26 See Banking and Financial Services Ombudsman, *Terms of Reference*, 1 December 2004, [3.1]; *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [4.1].

27 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159–160.

the expectations of the individuals concerned, so that individuals with complaints can continue to have their concerns dealt with effectively and efficiently'.[28]

Submissions and consultations

45.18 Stakeholders commented on the transfer of privacy complaints between complaint-handling bodies. The OPC explained that where it becomes aware that a privacy complaint is being handled by the BFSO or TIO, it will generally decline to investigate the matter concurrently on the basis that the respondent is engaged in a dispute resolution process that has yet to be finalised and, as such, has not had an adequate opportunity to deal with the matter.[29] The OPC suggested that it be given a specific power to decline to investigate in this situation. It also recommended that it be given the power to decline to investigate a complaint that would be handled more suitably by a recognised EDR scheme and to refer the complaint to the scheme with a request for investigation. The OPC suggested that these decline and referral powers could be limited to matters that are before a 'recognised' EDR scheme, and the OPC could be given the additional function of recognising such bodies for the purposes of the exercise of such powers.[30]

45.19 Other stakeholders commented on the role of EDR schemes. For example, Veda Advantage expressed support for a 'system of alternative dispute resolution that is speedy and informal' and noted that that it has joined the BFSO scheme.[31] Legal Aid Queensland submitted that EDR schemes monitored by a regulator can provide effective redress for complainants. For example, in the financial services sector, licensed entities must belong to an EDR scheme approved by the Australian Securities and Investments Commission (ASIC). Legal Aid stated that this requirement 'has provided positive outcomes for many thousands of consumers who were unable to access court based solutions'.[32]

ALRC's view

Transferring complaints to EDR schemes

45.20 The ALRC believes there is merit in recognising more formally the role of EDR schemes in handling privacy complaints. Schemes such as the TIO and BFSO already

---

28 Office of the Privacy Commissioner, 'Ombudsman and Privacy Commissioner to Streamline Joint Complaint Handling Processes' (Press Release, 30 November 2006).

29 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See *Privacy Act 1988* (Cth) s 41(2)(b).

30 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

31 Veda Advantage, *Submission PR 163,* 31 January 2007. See also Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

32 Legal Aid Queensland, *Submission PR 212,* 27 February 2007. The role of EDR schemes in the credit-reporting context is discussed in Ch 55.

resolve privacy complaints under their terms of reference and provide an efficient and binding avenue of complaint resolution for complainants and respondents.[33]

45.21 In the ALRC's view, the *Privacy Act* should be amended to empower the Commissioner to decline to investigate, or investigate further, a complaint that is already being handled by an approved EDR scheme. The Commissioner should also be empowered both to decline to investigate a complaint and refer it on to an EDR scheme, where the Commissioner is satisfied that the complaint would be handled more suitably by the scheme. A greater role for EDR schemes in dealing with privacy complaints has the potential to increase efficiency in dispute resolution and to provide parties with a one-stop-shop for complaints that are partly about privacy and partly about service delivery.

45.22 The ALRC notes that the EDR schemes under these proposed powers must be 'approved' by the OPC. This is consistent with the approach taken in Chapter 55, where the ALRC proposes that credit providers must be part of an 'approved EDR scheme' to be able to list default information. As noted in Chapter 55, the OPC could be expected to approve EDR schemes already approved by the ASIC under the *Corporations Act* and those with another statutory basis, such as the TIO.[34] In approving new schemes, the OPC could look at the ASIC standards and other similar instruments for benchmarks in its approval process.[35] The ALRC notes that the ASIC standard requires that approved EDR schemes report to ASIC on systemic issues and serious misconduct.[36] A similar reporting mechanism would be valuable in the privacy context to increase the OPC's awareness of systemic issues.

45.23 If these reforms were implemented, the OPC should publish a list of approved EDR schemes on its website, to increase transparency and awareness of the referral process.

Referring complaints to state bodies

45.24 The ALRC believes there can be similar benefits in using existing state complaint-handling bodies for the investigation and resolution of privacy complaints under the *Privacy Act*. This would facilitate complaints being handled by local bodies, which can be more efficient and convenient for the complaint handler and the parties to the complaint.

---

33 Under the Terms of Reference of the BFSO, a determination issued by the BFSO is binding on the complainant and respondent if the complainant agrees to accept it in full and final settlement of the subject matter of the dispute: Banking and Financial Services Ombudsman, *Terms of Reference*, 1 December 2004, [7.12]. A similar approach is taken by the TIO: *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.1].

34 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).

35 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999.

36 Ibid, [PS 139.59].

45.25 Two models are available under which this federal-state relationship could be set up. The first is to adopt intergovernmental arrangements similar to those under the *Human Rights and Equal Opportunity Act* (HREOC Act).[37] Under this model, the Minister may make an arrangement with a minister of a state or territory for or in relation to the performance on a joint basis of any functions of the Commissioner; or the performance by that state or territory or by an instrumentality of that state or territory on behalf of the Commonwealth of any functions of the Commissioner. The second option is to extend the Commissioner's delegation power under the *Privacy Act* to empower the Commissioner to delegate to a state or territory authority any of his or her powers in relation to complaint handling, including the power to issue determinations.[38]

45.26 There are advantages and disadvantages to both models. The first is more transparent and may provide an easier mechanism to put any necessary funding arrangements in place. The second option, however, may provide greater flexibility, as it would allow the Commissioner to delegate his or her powers on a case-by-case basis, without the need to set up formal arrangements.

45.27 The ALRC's preliminary view is that the Commissioner's delegation function should be extended. The ALRC understands that there have been difficulties in practice in implementing the HREOC arrangements. In the ALRC's view, flexibility is important to assist with the efficient and effective resolution of complaints. The ALRC notes that the Commissioner would not be required to delegate his or her functions unless of the view that it would be appropriate or effective to do so.

Guidance

45.28 Given the ALRC's proposals to empower the Commissioner to transfer complaints to EDR schemes and delegate complaint-handling powers to state bodies, it would be beneficial to provide guidance on these different avenues of complaint handling to agencies, organisations and potential complainants. This could be part of a document setting out the OPC's complaints handling policies and procedures.[39]

Proposal 45–2 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) decline to investigate a complaint where the complaint is being handled by an approved external dispute resolution scheme; or

37 See *Human Rights and Equal Opportunity Act 1986* (Cth) s 16.
38 The delegation power is set out in *Privacy Act 1988* (Cth) s 99.
39 See Proposal 45–8.

(b) decline to investigate a complaint that would be more suitably handled by an approved external dispute resolution scheme, and to refer that complaint to the external dispute resolution scheme with a request for investigation.

Proposal 45–3 Section 99 of the *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers, including a power conferred by section 52, in relation to complaint handling conferred on the Commissioner by the *Privacy Act*.

Resolution of privacy complaints

Model under the *Privacy Act*

45.29 The *Privacy Act* provides two formal ways of resolving a complaint following an investigation. First, the Commissioner can endeavour, by conciliation, to effect a settlement between the complainant and respondent.[40] Secondly, the Commissioner can make a determination either dismissing the complaint or finding the complaint substantiated.[41]

Conciliation

45.30 The Commissioner is given the general direction in complaints against both agencies and organisations, to attempt, by conciliation, to effect a settlement of the matters that gave rise to the investigation. The Commissioner is only required to conciliate a complaint where he or she considers it appropriate to do so.[42] In contrast to other privacy legislation, the *Privacy Act* does not set out detailed provisions on how to conduct the conciliation process.[43]

45.31 In practice, the OPC will conciliate complaints where it thinks there is enough evidence to support the complaint. The OPC conciliates by writing or telephoning the respondent to see if they agree to the complainant's solution, or bringing parties together in a conciliation conference.[44] If parties reach an agreement during conciliation, the OPC closes the file on the basis that the respondent has dealt adequately with the matter. The OPC received around 1200 complaints in 2005–06.[45]

---

40 *Privacy Act 1988* (Cth) ss 27(1)(a), 27(1)(ab).

41 Ibid s 52.

42 Ibid ss 27(1)(a), 27(1)(ab).

43 See, eg, the conciliation provisions in *Information Privacy Act 2000* (Vic) pt 5, div 3; *Health Records Act 2001* (Vic) pt 6, div 3; *Information Act 2002* (NT) ss 110–113 (in relation to mediation). See also the proposed provisions in Information Privacy Bill 2007 (WA) pt 5, div 2.

44 See Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

45 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 126.

Typical outcomes involved the respondent: apologising to the complainant; providing access to, or correcting, a record; changing its procedures; and paying compensation.[46]

45.32 If the parties cannot reach agreement during conciliation, the OPC will make a decision about how the complaint should be resolved. That decision may be that the respondent has made the complainant a reasonable offer which they have not accepted, in which case the OPC may close the file on the grounds that the respondent has dealt with the matter adequately, even if the complainant does not agree. Alternatively, the OPC may decide that the respondent has not made a reasonable offer, in which case the Commissioner can make a determination instructing the respondent on how to resolve the complaint, including by ordering the respondent to apologise, pay compensation or change its practices.[47]

Determinations

45.33 As noted above, the Commissioner can make a determination dismissing the complaint or can find a complaint substantiated and make a determination that includes one or more of the following declarations that:

- the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct;[48]
- the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;[49]
- the complainant is entitled to a specified amount by way of compensation for any loss or damage;[50] or
- it would be inappropriate for any further action to be taken in the matter.[51]

---

46 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), Table 3.4. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 126.

47 This is summarised from Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007.

48 *Privacy Act 1988* (Cth) s 52(1)(b)(i).

49 Ibid s 52(1)(b)(ii). 'Loss or damage' is defined in s 52(1A).

50 Ibid s 52(1)(b)(iii). The *Privacy Act* does not limit the monetary compensation that the Commissioner may award to a complainant: Australian Institute of Company Directors, Office of the Federal Privacy Commissioner and Information and Privacy Commissioner Ontario, *Privacy and Boards: What You Don't Know Can Hurt You* (2004), 11; *Rummery and Federal Privacy Commissioner* [2004] AATA 1221, [26]–[29]. See s 52(4)–(6) in relation to compensation orders in representative complaints. The Commissioner can also make a declaration that the complainant is entitled to a specified amount as reimbursement for expenses reasonably incurred in connection with the complaint: *Privacy Act 1988* (Cth) s 52(3).

51 *Privacy Act 1988* (Cth) s 52(1)(b)(iv).

45.34 A determination of the Commissioner under s 52(1) is not binding or conclusive between any of the parties to the determination.[52] This reflects the fact that Commonwealth judicial power can only be exercised by a court in accordance with Chapter III of the *Australian Constitution*.[53] Enforcement of determinations is discussed in Chapter 46.

45.35 There have been eight complaint determinations made since the *Privacy Act* commenced in 1989, with the most recent being in 2004.[54] Following a number of submissions from stakeholders commenting on the limited exercise of the determination power and suggesting that complainants should be able to compel the Commissioner to make a determination, the OPC Review recommended that it would consider circumstances in which it might be appropriate to make greater use of the Commissioner's power to make determinations under s 52.[55] Since then, the OPC has reviewed the use of the s 52 determination powers and identified situations where it may proceed more quickly to a determination, including where the:

- interests of the parties will be better served by the opportunity to make formal submissions to the Commissioner;
- issues in the complaint are not clear and the Commissioner will need to make findings; or
- complaint is not amenable to conciliation or conciliation has failed.[56]

45.36 The OPC also clarified that determinations would 'not necessarily be limited to the most serious cases, nor will determinations issued by the Commissioner necessarily be punitive'.[57]

45.37 The other issue with determinations identified by stakeholders in the OPC Review is the inability of the Commissioner to prescribe remedies to prevent future harm. The issue was said to be illustrated in determinations made against a residential tenancy database operator in 2004. In those determinations, the Commissioner found that, while he could declare that the respondent should not repeat or continue conduct

---

52 Ibid s 52(1B).

53 C Saunders, 'The Separation of Powers' in B Opeskin and F Wheeler (eds), *The Australian Federal Judicial System* (2000) 3, 14, 15–16, 25. See, eg, *Huddart, Parker & Co Pty Ltd v Moorehead* (1909) 8 CLR 330, 357; *Waterside Workers' Federation of Australia v JW Alexander Ltd* (1918) 25 CLR 434, 442; *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254, 281–282; *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245.

54 Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 1 August 2007.

55 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 42, 37. See also the discussion at 139, 144.

56 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2.

57 Ibid, 2.

that constitutes an interference with the privacy of an individual, he did not have the power to prescribe how the respondent should act in the future.[58] Following concerns from stakeholders that this restriction limited the Commissioner's ability to address systemic issues, the OPC recommended that the Government consider amending the *Privacy Act* to expand the remedies available under a determination to include giving the Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues.[59] In its response to the OPC Review, the Australian Government agreed with this recommendation.[60]

Submissions and consultations

Framework for conciliation

45.38 Stakeholders expressed concerns about the lack of distinction between the stages of investigation, conciliation and determination under the *Privacy Act*.[61]

45.39 The OPC commented on the timing of conciliation in the complaint-handling process. The OPC noted that s 27 provides for a complaint to be conciliated *after* investigation. The OPC expressed interest in 'promoting early conciliation, where appropriate, as an expedient means of resolving complaints to the satisfaction of both parties'. It recommended that its specific conciliation functions in s 27 be amended to provide for the option of conciliating complaints at any stage in the complaint-handling process, including before the commencement of a formal investigation.[62]

45.40 Stakeholders commented on the fact that the Commissioner may stop investigating a complaint if he or she is satisfied that the respondent has dealt adequately with the complaint, even if the complainant does not agree.[63] The CCLC noted that:

> In the last reported year, the most commonly cited reason for declining to investigate complaints further following an investigation was made under s 41(2)(a) of the Act, ie that the respondent had adequately dealt with the matter. CCLC's advice and casework experience has revealed that this response from the OPC has frustrated

---

58 See Office of the Federal Privacy Commissioner, *Complaint Determination No 1 of 2004*, 1 April 2004. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 136.

59 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 44.

60 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), [Item 44].

61 Veda Advantage, *Submission PR 163,* 31 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

62 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

63 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

> many consumers, and as illustrated by *X v Commonwealth Agency* [2004], a dismissal of complaints on these grounds stands even if the complainant does not agree.[64]

45.41 The Australian Privacy Foundation submitted that the conciliation process adopted by the OPC, which involves the 'exchanges of correspondence over lengthy periods', is inefficient and ineffective.[65] Similarly, the CCLC submitted that the OPC's 'conciliatory approach does not necessarily produce fair results' as the delay in conciliating the complaint can deter one party from continuing, rather than acting to further negotiation.[66] In contrast, the Australian Federal Police submitted that it 'is able to work within the current privacy complaint handling system'.[67]

45.42 The Australian Government Department of Human Services expressed concern that the *Privacy Act* does not protect adequately the conciliation process, as there is 'no provision for confidentiality where conciliation is being or has been pursued'.[68]

Exercise of determination power

45.43 Several stakeholders commented on the very limited use of the determination power and the fact that successive Commissioners have failed to use the power, even when requested to do so by complainants.[69] The Australian Privacy Foundation explained that the 'determination making powers are potentially very powerful' and noted its experience that

> many complainants desire, more than anything else, a formal finding that the respondent has breached a privacy principle. Greater use of the determination making powers would also result in a body of public decisions which would be a valuable resource for educating both data users and the public about the application of the law, and which could if necessary be formally challenged in the courts.[70]

45.44 The Commonwealth Ombudsman expressed the view that the 'apparent intent of the *Privacy Act* is that most matters will be resolved between the complainant and the respondent, but with some guidance from the Commissioner and the determinative role of the Commissioner standing as an inducement for settlements'.[71] The Legal Aid Commission of NSW submitted that the rarity of formal determinations by the Commissioner was understandable, 'given the emphasis on conciliation of complaints

---

64 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
65 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
66 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
67 Australian Federal Police, *Submission PR 186,* 9 February 2007.
68 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007. See also Veda Advantage, *Submission PR 163,* 31 January 2007.
69 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
70 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
71 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.

and the limited legal consequences of determinations that do not include a finding substantiating a complaint'.[72]

45.45 The Office of the NSW Privacy Commissioner (Privacy NSW) submitted that it is not clear how or in what circumstances the Commissioner may elect to use the determination power. It suggested that the internal review process prescribed by the *Privacy and Personal Information Act 1998* (NSW) provided a more successful mechanism to resolve complaints efficiently.[73]

45.46 Stakeholders submitted that, given the current power for the Commissioner to dismiss complaints when he or she is satisfied that the respondent has dealt adequately with the matter, even if the complainant does not agree, complainants should have the right to compel a determination under s 52 of the Act.[74] One stakeholder pointed to the fact that, at the very least, a determination can contain a public declaration that the respondent breached the privacy principles. If a complainant does not agree with declarations made in a determination, such as the adequacy of compensation, a determination gives rise to other rights, including merits review in the Administrative Appeals Tribunal (AAT) and a hearing in the federal courts. Even if the determination dismissed the complaint, the complainant would have a more detailed decision upon which to found an action for judicial review.[75]

45.47 In contrast to these submissions, the Law Council Privacy Working Party suggested that the Commissioner's powers to make determinations are appropriate and administered effectively and the 'light touch' approach to privacy protection 'strikes an acceptable balance between consumer rights and efficiency in business'. The Working Party did not support a right to compel determinations, submitting that the ability of the Commissioner to dismiss frivolous and vexatious complaints at an early stage promotes flexibility and efficiency by reducing costs associated with unnecessary investigations. It also provides an incentive for respondents to deal independently with complaints to avoid a formal determination. In contrast, public disclosure of privacy breaches in a determination, even where the complainant had addressed the breach adequately, would discourage respondents from 'taking independent action to resolve these issues'.[76]

---

72 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

73 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007. See *Privacy and Personal Information Protection Act 1998* (NSW) pt 5.

74 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. Legal Aid Queensland also supported the right for a complainant to compel the Commissioner to make a determination: Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

75 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. See also Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

76 Law Council of Australia, *Submission PR 177,* 8 February 2007.

45.48 Legal Aid Queensland also considered the incentive for organisations to resolve complaints. Its view, however, was that corporations are 'very aware' that the Commissioner rarely makes determinations and 'in such circumstances, there is no incentive on corporations to commercially resolve the matter'.[77]

Addressing systemic issues

45.49 Several stakeholders, including the OPC, suggested that the Commissioner's determination powers should be amended to allow the Commissioner to prescribe remedies for systemic issues.[78] For example, AAMI submitted that

> the Commissioner does not have enough legislative power to be able to deal with systemic issues within industry. The OPC currently acts as more of an Ombudsman rather than a Regulator. This shortfall does not benefit the consumer as individual complaints have to be made against each organisation in turn if a systemic issue is to be rectified.[79]

45.50 The Australian Privacy Foundation noted that the determination power does not appear to allow the Commissioner to prescribe acceptable acts and practices, giving the example of the 2004 residential tenancy database determinations, discussed above. The Foundation submitted that the Commissioner's finding that he could not prescribe what steps the respondent should take left enforcement as a 'guessing game' and it was 'clearly desirable' that this situation be clarified by amending s 52 to include an ability to prescribe acceptable acts and practices.[80] Privacy NSW also supported giving the Commissioner the power to require a respondent to obey orders requiring prescriptive action. Privacy NSW considered that this would allow the Commissioner 'to specify, as part of the determination orders, positive and prescriptive actions to be taken to improve an agency or organisation's level of statutory compliance'.[81]

ALRC's views

Framework for conciliation and determinations

45.51 The relationship in the *Privacy Act* between conciliation and determination is not clear. An explanation of the intended relationship was provided in the Second Reading Speech for the Privacy Bill 1988 (Cth), where the then Attorney-General stated:

---

77 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

78 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; AAMI, *Submission PR 147,* 29 January 2007. See also Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 44.

79 AAMI, *Submission PR 147,* 29 January 2007.

80 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

81 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

> Under the Bill an individual will be able to complain to the Privacy Commissioner about alleged interferences with privacy, who will attempt to resolve the allegations by conciliation and, failing that, making binding determinations against agencies, including determinations for compensation and costs.[82]

45.52 The ALRC believes that the relationship between conciliation and determination, and the Commissioner's functions in relation to each, should be clarified in the *Privacy Act* to provide greater transparency and accountability. First, the ALRC proposes that s 27(1)(a) and (ab) be amended to clarify up front the Commissioner's various functions in relation to privacy complaints, including the functions of receiving and investigating complaints, conciliating where appropriate or making a determination. Consistently with the proposal that the *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity,[83] this amendment would, if implemented, provide a succinct summary of the Commissioner's functions in relation to the investigation and resolution of privacy complaints. It would also clarify the Commissioner's ability to conciliate a complaint at any stage after receiving it.[84]

45.53 Secondly, the ALRC proposes that the *Privacy Act* be amended to include new provisions dealing expressly with conciliation. These provisions should clarify that the Commissioner must use all reasonable attempts to conciliate a complaint where the Commissioner thinks it reasonably possible that the complaint may be conciliated successfully. This expands on the existing obligation on the Commissioner in s 27 to conciliate complaints where appropriate, and is similar to obligations on privacy commissioners in other privacy legislation.[85]

45.54 Thirdly, the provisions should clearly set out what happens when conciliation fails. The ALRC proposes that conciliation will be taken to have failed where, in the opinion of the Commissioner, all reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation. This framework adopts language from industrial relations legislation, where conciliation and

---

82 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). A similar description of the role of conciliation and determinations was given in Explanatory Memorandum, Privacy Bill 1988 (Cth), 3. Note determinations were originally automatically binding between parties, before the amendments made by the *Law and Justice Amendment Act 1994* (Cth) and the *Human Rights Legislation Amendment Act 1995* (Cth).

83 Proposal 3–2.

84 Note there is precedent for a more open conciliation power in the *Anti-Discrimination Act 1977* (NSW) s 91A, which provides that the President may 'at any stage after acceptance of the complaint endeavour to resolve the complaint by conciliation'. The ability of the Commissioner to conciliate the complaint at any stage is also reflected in Proposal 45–5(a).

85 See *Information Privacy Act 2000* (Vic) s 33; *Health Records Act 2001* (Vic) s 59. See also the precedent in *Industrial Relations Act 1996* (NSW) s 109.

arbitration are well-established practices in resolving industrial disputes.[86] State and territory privacy legislation also provides expressly for conciliation failing or being unsuccessful.[87] This amendment would, if implemented, provide clearer parameters in which to conduct conciliation.

45.55 Finally, the ALRC proposes that the Act should be amended to provide that where the Commissioner is of the opinion that conciliation has failed, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

45.56 This proposal is analogous to the provisions in the *Information Privacy Act 2000* (Vic), where, if the Commissioner has attempted unsuccessfully to conciliate a complaint, he or she must notify the complainant and the respondent in writing, and the complainant may require the Commissioner to refer the complaint to the Victorian Civil and Administrative Tribunal for hearing.[88] It is also comparable to the approach in the HREOC Act where, if the President terminates a complaint on the basis that he or she is satisfied that there is no reasonable prospect of the matter being settled by conciliation, any person affected in relation to the complaint may make an application to the Federal Court or the Federal Magistrates Court alleging unlawful discrimination by the respondent.[89] The ALRC's proposed model is also similar to the relationship between conciliation and arbitration in state industrial relations legislation.[90]

45.57 This proposal, if implemented, should lead to an increase in the number of determinations issued by the OPC, which would help address concerns from stakeholders about the lack of jurisprudence on the *Privacy Act*.[91] The proposal should increase public enforcement and awareness of the Act, which is consistent with Parliament's expectation that the Commissioner 'be the means by which there will be accountability to the public on the use by government of their personal information'.[92] The proposal is also consistent with the legislative intention that determinations be

---

86 See, eg, *Industrial Relations Act 1996* (NSW) ss 134–135.

87 See *Information Privacy Act 2000* (Vic) s 37; *Health Records Act 2001* (Vic) s 63; *Information Act 2002* (NT) s 111.

88 *Information Privacy Act 2000* (Vic) s 37. See also *Health Records Act 2001* (Vic) s 63; *Information Act 2002* (NT) s 113.

89 *Human Rights and Equal Opportunity Act 1986* (Cth) ss 46PH(1)(i), 46PO.

90 See *Industrial Relations Act 1996* (NSW) s 135.

91 The ALRC considers that there is greater jurisprudential value in determinations than in case notes of conciliated complaints. Professor Julia Black has argued that, as settlements represent a compromise on both sides, the 'dynamics of a settlement negotiation are not conducive to a pure and objective interpretation and application of principles'. As such, it can be difficult to know how far a particular interpretation adopted in a conciliated case 'is applicable in other factual situations, whether directly or by analogy': J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 15–16.

92 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (L Bowen–Attorney-General). Note this speech only refers to the government, as organisations were not covered by the *Privacy Act* when the Act was originally passed.

issued where conciliation has failed. The presence of the power to request a determination should provide a real incentive for agencies and organisations to engage in the conciliation process, which some stakeholders suggest has been lost due to the very limited number of determinations issued.

45.58 The ALRC acknowledges the concerns raised by stakeholders that providing a right to compel a determination may encourage vexatious litigants and may add to the unreasonable expectations sometimes held by complainants about how a complaint will be resolved. The model proposed by the ALRC, however, incorporates adequate safeguards against vexatious and trivial conduct, as it only operates in relation to complaints that the Commissioner has not dismissed under s 41. That is, the complaint must have passed the threshold requirements of being in time, involving a possible breach, and not being frivolous, vexatious, misconceived or lacking in substance. The complaint must, therefore, have a degree of merit. The proposal also requires the complainant and respondent to have made a genuine and concerted effort to conciliate the complaint.

45.59 The ALRC also proposes that the Act be amended to protect evidence produced in the conciliation process from being used in a determination hearing or later enforcement proceedings. This proposed provision is based on a provision in the Victorian *Information Privacy Act,*[93] and is intended to encourage parties to engage in full and frank negotiations as part of conciliation.

Addressing systemic issues

45.60 The ALRC recognises the need for the Commissioner to be able to prescribe remedies that address systemic issues and effect systemic changes in agencies, organisations and industries. The ALRC proposes that the Commissioner's determination powers under s 52 be amended to empower the Commissioner to make an order in a determination that a respondent must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*.[94] The ability to prescribe how the respondent should act to comply with, for example, the proposed Uniform Privacy Principles (UPPs) should end the enforcement 'guessing game' described by stakeholders. It should also provide greater certainty to agencies, organisations and the public on what behaviour is consistent with the principles or regulations.[95]

---

93 See *Information Privacy Act 2000* (Vic) s 36.

94 This wording is based on the compliance notice model used in other privacy legislation. See Ibid s 44; *Health Records Act 2001* (Vic) s 66; *Information Act 2002* (NT) s 82.

95 Greater certainty was requested by some residential tenancy database operators following the 2004 determinations: see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.

45.61 The ALRC notes that the proposal to give complainants and respondents a right to require the Commissioner to resolve a complaint by determination in certain circumstances should, in conjunction with the proposal to empower the Commissioner to prescribe steps a respondent must take to bring itself into compliance with the Act, help effect systemic change. While a determination may relate to an individual complaint, that individual complaint may itself be about a systemic issue.[96] Empowering the Commissioner to prescribe remedies that are able to address systemic issues in the complaint handling process allows the Commissioner to achieve maximum change from each individual complaint.

Proposal 45–4 Sections 27(1)(a) and (ab) of the *Privacy Act* should be amended to make it clear that the Privacy Commissioner's functions in relation to complaint handling include:

(a) to receive complaints about an act or practice that may be an interference with the privacy of an individual;

(b) to investigate the act or practice about which a complaint has been made; and

(c) where the Commissioner considers it appropriate to do so and at any stage after acceptance of the complaint, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint or to make a determination in respect of the complaint under s 52.

Proposal 45–5 The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following:

(a) If, at any stage after receiving the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make all reasonable attempts to conciliate the complaint.

(b) Where, in the opinion of the Commissioner, all reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

96 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999, [PS 139.131]–[PS 139.133]. An example of such a complaint is provided in *D v Banking Institution* [2006] PrivCmrA 4.

(c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.

Proposal 45–6 Section 52 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make an order in a determination that an agency or respondent must take specified action within a specified period for the purpose of ensuring compliance with the Act.

Accountability and transparency

Background

45.62 A number of stakeholders have submitted that transparency and accountability in complaint handling under the *Privacy Act* should be improved. Two methods to improve transparency and accountability are merits review of the Commissioner's determinations and providing more guidance on the OPC's complaint-handling policies and procedures.

Merits review

Background

45.63 The right to merits review of determinations made by the Commissioner is limited to where the respondent is an agency, and is available only in relation to the Commissioner's decision to include or not include a declaration for compensation or costs.[97] There is no right of appeal to the AAT in respect of determinations against organisations or determinations dismissing a complaint.

45.64 Some stakeholders making submissions to the OPC Review expressed the view that the narrowness of merits review available under the *Privacy Act* is one factor that prevents there being a useful legal jurisprudence on the Act which people can rely on.[98] It was suggested that the existing provisions were unfair to complainants because, while respondents have a de facto right to have the case heard afresh by refusing to comply with a determination and waiting for the Commissioner or complainant to enforce it in court, this strategy is not available to an aggrieved complainant.[99] The OPC Review concluded that the lack of merits review of determinations was out of step with the position applying to other government authorities and recommended that

97 *Privacy Act 1988* (Cth) s 61.

98 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 137–138.

99 Ibid, 138–139. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

the Government amend the Act 'to give complainants and respondents a right to have the merits of complaint decisions made by the Commissioner reviewed'.[100]

Submissions and consultations

45.65 A number of stakeholders supported a right to merits review of complaint determinations involving organisations.[101] Some described the lack of appeal rights as the 'principal deficiency in the Act'.[102] The Legal Aid Commission of NSW suggested that the key issue with determinations is the absence of a right of appeal against a determination by the Privacy Commissioner under s 52(1)(a) dismissing a complaint. It suggested that 'the lack of such an appeal removes an important accountability check on the way the Commissioner's investigative functions operate' and that the alternative course of a review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) is limited and does not allow the merits of the decision to be assessed adequately.[103]

45.66 The OPC expressed support for 'the extension of the appeal rights under the *Privacy Act* in the interests of providing a fair and transparent complaint-handling process that is sufficiently open to scrutiny'.[104] It recommended that all determinations made by the Commissioner should be reviewable by the AAT, including those made against organisations. The review, it was suggested, should extend to all decisions made using the determination power, rather than being limited to decisions regarding compensation.[105]

45.67 Privacy NSW suggested that merits review would assist in dealing with the problem that determinations are not binding and would remove the necessity of taking determinations to the Federal Court for enforcement.[106] In contrast, the Queensland Council for Civil Liberties failed to see the need for AAT merits review and submitted

---

100 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 153, rec 40.

101 Queensland Government, *Submission PR 242,* 15 March 2007; Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Telstra, *Submission PR 185,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

102 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

103 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

104 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

105 Ibid.

106 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

that the process of seeking enforcement through the courts would 'no doubt effectively act as a review'.[107]

ALRC's view

45.68 The ALRC believes the current rights to merits review of determinations are not sufficient. To increase transparency and accountability, and to facilitate the growth of more jurisprudence on the *Privacy Act*, the ALRC proposes that the Act be amended to provide for merits review of all decisions made by the Commissioner under s 52.

Proposal 45–7 The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner under s 52 and the current review rights set out in s 61 should be repealed.

Complaint-handling policies and procedures

Background

45.69 Another method of increasing transparency and accountability in the OPC's processes and decision making is by publishing clear policies and procedures that outline how the OPC deals with complaints, and by publishing case notes.

45.70 Submissions from stakeholders calling for the OPC to produce a comprehensive manual on its complaint resolution policies and procedures, in order to shed more light on the way it handles complaints, were considered in the OPC Review.[108] The OPC Review recognised that greater transparency was likely to benefit both complainants and respondents and would increase scrutiny of the OPC's decisions. It found, however, that 'it does not appear to be common practice for regulators to publish manuals which set out in great detail their complaint processes'.[109]

45.71 Case notes can help add transparency and accountability to the OPC's handling of complaints by providing examples of how the principles have been interpreted and applied in practice. The OPC publishes case notes that describe the issues and outcomes in selected complaints and has stated that, by providing this insight into how the privacy principles are being applied, the Commissioner aims to 'ensure the Office

---

107 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

108 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 137, 142, 151.

109 Ibid, 151.

is accountable and transparent in its processes and decision making'.[110] Case notes also play an important role in promoting individual privacy, as they 'serve to demonstrate to members of the public how the Commissioner handles complaints' and they 'assist the public to know if their personal information is being handled appropriately, or assist them to decide whether to pursue a complaint'.[111]

Submissions and consultations

45.72 Several stakeholders commented on the lack of transparency and accountability in the OPC's complaint-handling procedures.[112] One stakeholder submitted:

> There is no published manual of the procedures used, and policies adopted, by the OPC in its investigation and resolution of complaints. Potential complainants, respondents and organizations representing them, are left to infer these procedures and policies from piecemeal and scattered complaint summaries which are infrequently issued by the OPC.[113]

45.73 Stakeholders commented on the lack of transparency about complaint resolutions and the remedies being granted by the OPC.[114] For example, it was noted that while the OPC has improved the level and detail of its case note reporting, it 'is still not sufficient to play the role that reporting of examples can and should play in the overall administration of the *Privacy Act*'.[115] In particular, stakeholders pointed to the lack of understanding of the criteria the OPC applies in deciding which cases to report, and the fact that there is 'no objective means of measuring whether these are a true reflection' of the OPC's practices.[116]

45.74 Stakeholders also noted the lack of transparency around how the OPC screens complaints in the initial stages, which 'makes it difficult for organisations to ensure they prepare and consult in the appropriate manner'.[117] Similarly, the Institute of Mercantile Agents suggested that 'every complaint should generate an advice to all

---

110 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 41. See Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 1 August 2007.

111 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 4, 41. See Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

112 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

113 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

114 Ibid; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

115 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

116 Ibid.

117 AAMI, *Submission PR 147,* 29 January 2007.

parties so an investigation can be commenced immediately and all information needed is protected and not deleted'.[118]

45.75 Two methods were put forward by stakeholders to remedy this lack of transparency. The first was that guidelines or a manual setting out the OPC's complaint-handling policies and procedures should be published.[119] For example, the Department of Human Services submitted:

> Guidelines should be developed for the investigation and conciliation processes that clearly articulate roles and responsibilities. The guidelines should include information regarding confidentiality during all phases of the investigation as well as appropriate provision of relevant information to the Privacy Commissioner.[120]

45.76 The second method suggested—often in addition to publishing a complaint-handling manual—was to require the Commissioner to publish more case notes.[121] For example, one stakeholder submitted that the OPC should reform its procedures for reporting privacy complaints and should, among other things, adhere to publicly-stated criteria of seriousness in deciding which complaints to report.[122]

45.77 Increasing efficiency in administering the Act by reducing delay in resolving privacy complaints was a related concern. The issue of delay in investigating and resolving privacy complaints was of great concern to many stakeholders—consumers, organisations and agencies alike.[123] The OPC received a boost of $8.1 million in additional funding in the 2006 budget. In its 2005–06 Annual Report, the Commissioner indicated that one of the major areas to which the additional funding

---

118 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

119 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

120 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

121 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007. Stakeholders to the OPC Review also called for the publication of more case notes: Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 142–143, 151–152.

122 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. See also G Greenleaf, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 20 December 2004 as affirmed in Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

123 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007; Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AXA, *Submission PR 119,* 15 January 2007; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; Commonwealth Ombudsman, *Consultation PC 11*, Canberra, 30 March 2006. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

would be directed was complaint handling. This would allow the OPC to handle privacy complaints efficiently and 'reduce the current complaint backlog while enhancing service standard and conciliating techniques'.[124]

ALRC's view

45.78 The ALRC believes that a valuable way to increase transparency in complaint handling under the *Privacy Act* would be for the OPC to prepare and publish a document setting out its complaint-handling policies and procedures. This document could draw on existing resources and publications of the OPC, such as information included in the 'Privacy Complaints' section on the OPC website and in Information Sheet 13, which sets out the Commissioner's approach to promoting compliance with the *Privacy Act*.[125] The proposed document could also include the OPC's new determination policy.[126]

45.79 Consolidating this information into one document should increase the accessibility and transparency of the complaint-handling process. It would also make a useful resource for agencies, organisations and individuals.

Proposal 45–8 The Office of the Privacy Commissioner should prepare and publish a document setting out its complaint-handling policies and procedures.

Other issues in the complaint-handling process

Background

45.80 In addition to general issues about investigation and resolving complaints under the *Privacy Act*, stakeholders raised a number of concerns relating to specific provisions in the Act. These included those provisions dealing with representative complaints, preliminary inquiries, and the conduct of investigations.

Representative complaints

45.81 The *Privacy Act* allows for the making of representative complaints, whereby one of a class of two or more individuals makes a complaint on behalf of all the

---

124 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 2. The ALRC also notes that the OPC has recently committed to new response timeframes for complaint handling: see Office of the Privacy Commissioner, 'Privacy Commissioner implements new response timeframes' (2007) 1(3) *Privacy Matters* 5.

125 See Office of the Privacy Commissioner, *Privacy Complaints* <www.privacy.gov.au/privacy_rights/complaints/index.html> at 1 August 2007; Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001).

126 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2.

individuals in the class.[127] A representative complaint can be lodged under s 36 if the class members have complaints against the same person; all the complaints are in respect of, or arise out of the same or related circumstances; and all the complaints give rise to a substantial common issue of law or fact.[128]

45.82 The Commissioner has power to determine that a complaint should no longer be treated as a representative complaint, and may turn an individual complaint into a representative complaint.[129] The Commissioner can also replace the complainant with another class member and a class member can withdraw from a representative complaint at any time before the Commissioner begins to hold an inquiry into the complaint. Representative complaints can be lodged without the consent of class members and a person who is a class member for a representative complaint is not entitled to lodge a complaint in respect of the same subject matter.[130]

Submissions and consultations

45.83 In Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the procedures for making and pursuing complaints, including representative complaints, are appropriate.[131] The OPC raised several issues about representative complaints in its submission to the ALRC. First, the OPC observed that there is no requirement that the party making a representative complaint has standing to make the complaint.[132] While noting that the Commissioner has certain discretions under the Act to cease handling a matter as a representative complaint, the OPC considered that it might be appropriate to provide the Commissioner with a specific discretion to refuse to handle a matter as a representative complaint where the party making the complaint has insufficient standing.[133]

45.84 Secondly, the OPC observed that an individual's capacity to make an individual complaint could be removed without their knowledge or agreement, by virtue of the combination of ss 38(3) and 39 of the *Privacy Act*. The only way an individual can retain the ability to make an individual complaint on the same topic is to withdraw from the representative complaint. The OPC recommended that individuals be given the option of 'opting out of a representative complaint at any time if the individual did not consent to be a class member'. The OPC noted, in this context, that the HREOC

127 *Privacy Act 1988* (Cth) s 36(2).
128 Ibid s 38(1).
129 Ibid ss 38A, 38C.
130 Ibid ss 38, 39.
131 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–12.
132 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
133 Ibid.

Act allows a class member to withdraw from a representative complaint at any time before the President terminates the complaint.[134]

45.85 The Australian Privacy Foundation suggested that 'Commissioners have not encouraged or used the potential of representative complaints' and that representative complaints are not 'given the attention they may deserve'.[135]

ALRC's view

45.86 In the ALRC's view, the *Privacy Act* should be amended to allow a class member of a representative complaint to withdraw from the complaint at any time if the class member has not consented to be a class member. This would address the issue that an individual's right to lodge a complaint can be removed by circumstances beyond their knowledge or control.

45.87 In relation to the issue of standing, s 38A gives the Commissioner a broad discretion to determine that a complaint should not continue as a representative complaint when he or she is satisfied that it is in the interests of justice to so. Reasons for making such a determination include that the complaint was not brought in good faith as a representative complaint, or where it is otherwise inappropriate that the complaints be pursued by means of a representative complaint.[136] These powers provide the OPC with adequate discretion to cease handing a complaint as a representative complaint where it was brought by a person with no standing.[137]

Proposal 45–9 Section 38B(2) of the *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member has not consented to be a class member.

Preliminary inquiries

45.88 Where a complaint is made to, or accepted by, the Commissioner, he or she has the power to make preliminary inquiries of the respondent. The power is limited by its purpose, which is to determine whether the Commissioner has power to investigate the matter complained about or whether the Commissioner may exercise his or her discretion not to investigate the matter.[138]

---

134 Ibid. The OPC noted the precedent in the *Human Rights and Equal Opportunity Act 1986* (Cth) s 46PC. Tthe HREOC Act's provisions on representative complaint are very similar to the *Privacy Act* and allow a representative complaint to be lodged without the consent of class members: *Human Rights and Equal Opportunity Act 1986* (Cth) s 46PB(4).

135 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

136 *Privacy Act 1988* (Cth) s 38A(2)(c)–(d).

137 See also Australian Law Reform Commission, *Beyond the Door-Keeper: Standing to Sue for Public Remedies*, ALRC 78 (1996).

138 *Privacy Act 1988* (Cth) s 42.

Submissions and consultations

45.89 The OPC suggested that the Commissioner should be given a specific power to contact third parties when undertaking preliminary inquiries into a complaint. This is particularly relevant when the complaint relates to a disputed credit default, in which case 'it is usually relevant to the assessment of the case for the Office to seek a copy of the individual's credit information file'. The OPC submitted that while it has the power to do anything 'incidental or conducive to the performance of any of the Commissioner's other functions', it would be appropriate for the Commissioner to have a specific power to contact third parties in these circumstances.[139]

ALRC's view

45.90 The ALRC's view is that s 42 of the *Privacy Act* should be amended to allow the Commissioner to contact third parties at the preliminary inquiries stage. While it is possible that a similar result could be achieved through the Commissioner's ancillary function to do anything 'incidental or conducive to the performance of any of the Commissioner's other functions', the ALRC believes that it would be clearer and more transparent if the section itself provided specifically that the Commissioner has the ability to make inquiries of third parties. This amendment should also help reduce delays in addressing complaints in the credit reporting context.

Proposal 45–10 Section 42 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make preliminary inquiries of third parties as well as the respondent.

Ceasing investigations if certain offences have been committed

45.91 If the Commissioner forms the opinion, in the course of an investigation, that a 'credit reporting offence' or 'tax file offence' has been committed, he or she must inform the Commissioner of Police or the Commonwealth Director of Public Prosecutions (DPP), and is to discontinue the investigation except to the extent that it concerns matters unconnected with the alleged offence. The Commissioner may continue with the investigation upon receiving a notice from the Commissioner of Police or the DPP indicating that the matter will not, or will no longer be, the subject of proceedings for an offence.[140]

---

139 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

140 *Privacy Act 1988* (Cth) s 49. An example of the operation of this provision is provided in *F and G v Taxation Accountant* [2006] PrivCmrA 6.

Submissions and consultations

45.92 The OPC noted that, in its experience, very few matters referred by the OPC to the Australian Federal Police (AFP) are prioritised for investigation. As the OPC's investigation is suspended while the AFP decides whether to investigate, this can cause delay in resolving the complaint. The OPC suggested that a way to alleviate these problems would be for the 'offence provisions to set a higher test than the test for an interference with privacy under the *Privacy Act*', thereby giving the OPC a kind of discretion not to refer a matter to the AFP where the conduct was not serious or caused no harm. While most of offences under the Act already set a higher test than for an interference with privacy (see, for example, s 18R), the exception is the tax file number offence under s 8WB of *Taxation Administration Act*.[141]

ALRC's view

45.93 The ALRC does not propose any reform to s 49 of the *Privacy Act*. While the ALRC acknowledges the operation of this provision can cause delays to the OPC's investigation, the referral of offences to the AFP and DPP is part of the broader prosecution policy of the Commonwealth.[142] The ALRC also proposes, in Part G, the repeal of the credit reporting offences.[143]

Conduct of investigations

45.94 The *Privacy Act* outlines how an investigation is to be conducted. As a general rule, an investigation is to be 'conducted in private but otherwise in such manner as the Commissioner thinks fit'.[144] The Commissioner must inform parties when an investigation commences or ceases.[145] For the purposes of performing the Commissioner's functions in relation to a complaint (except an NPP complaint or a code complaint accepted under s 40(1B)), the Commissioner can compel the complainant, respondent and any other relevant person to attend a conference.[146] The Commissioner also has the power, subject to certain limitations, to obtain information and documents from persons, and make inquiries of persons or examine witnesses on oath or affirmation.[147]

---

141 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

142 In particular, see Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (1992). The AFP also prioritises matters for investigations pursuant to its Australian Federal Police, *Case Categorisation and Prioritisation Model* (2006). Section 8WB of the *Taxation Administration Act* is currently under review by the Australian Government Treasury as part of the inquiry into secrecy and disclosure provisions in Australian taxation law: see Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006).

143 See Proposal 55–8.

144 *Privacy Act 1988* (Cth) s 43(2).

145 Ibid ss 43(1), 48.

146 Ibid s 46(1). It is an offence to fail to attend such a conference as required by the Commissioner: *Privacy Act 1988* (Cth) s 46(2).

147 *Privacy Act 1988* (Cth) ss 44–46. It is an offence not to comply with the Commissioner's directions: *Privacy Act 1988* (Cth) ss 46(2), 65–66.

45.95 In addition to these requirements, the *Privacy Act* requires that complainants and respondents be given the opportunity to appear before the Commissioner in certain circumstances. In particular, the Commissioner must not make a finding under s 52 that is adverse to a complainant or respondent unless the Commissioner has afforded the complainant and respondent an opportunity to appear before the Commissioner and to make submissions orally, in writing, or both, in relation to the matter to which the investigation relates.[148] This requirement reflects the 'hearing rule' which, in the context of administrative decision making, is the common law rule that a statutory authority having power to affect the rights of a person is bound to afford the person a hearing before exercising the power.[149]

45.96 The rules of natural justice, including the hearing rule, can be modified or abrogated by statute.[150] For example, the *Social Security (Administration) Act 1999* (Cth) provides that a party to a merits review of a decision before the Social Security Appeals Tribunal may make oral or written submissions, or both.[151] The Executive Director of the Social Security Appeals Tribunal may direct, however, that a hearing be conducted without oral submissions from the parties if: the Executive Director considers that the review hearing could be determined fairly on the basis of written submissions by the parties; and all the parties to the review consent to the hearing being conducted without oral submissions.[152]

45.97 The *Administrative Appeals Tribunal Act 1975* (Cth) provides that a matter may be dealt with by considering documents or other material lodged with or provided to the AAT—and without holding a hearing—if it appears to the AAT that the issues for determination on the review of a decision can 'be adequately determined in the absence of parties; and the parties consent to the review being determined without a hearing'.[153]

Submissions and consultations

45.98 In IP 31, the ALRC asked whether the Commissioner's powers relating to the conduct of investigations are appropriate and exercised effectively.[154] The Australian Privacy Foundation suggested that the Commissioner's investigation powers are generally appropriate but are not always exercised effectively.[155]

---

148 *Privacy Act 1988* (Cth) ss 43(4)–(5).

149 See R Creyke and J McMillan, *Control of Government Action: Text, Cases & Commentary* (2005); *Twist v Council of the Municipality of Randwick* (1976) 136 CLR 106, 110.

150 *Kioa v Minister for Immigration and Ethnic Affairs* (1985) 159 CLR 550.

151 *Social Security (Administration) Act 1999* (Cth) s 161.

152 Ibid s 162.

153 *Administrative Appeals Tribunal Act 1975* (Cth) s 34J. Note that s 76 of the *Administrative Decisions Tribunal Act 1997* (NSW) gives the Tribunal power to determine proceedings without holding a hearing if the Tribunal believes the issues can be adequately determined in the absence of the parties.

154 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–15.

155 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

45.99 The OPC supported the continued inclusion of the Commissioner's investigation powers provided in ss 43–47 of the *Privacy Act*. The OPC noted that these provisions relate to more extreme situations where agencies or organisations do not cooperate in the investigation process.[156] The OPC recommended, however, two changes to the provisions. First, it suggested that the references to a 'compulsory conference' in ss 46 and 47 be clarified to make it clear that it means a compulsory *conciliation* conference. Secondly, the OPC recommended that the power to compel parties to a compulsory conference should extend to NPP and code complaints. It observed that the Commissioner otherwise has the same functions in handling the different types of complaints (such as IPP, credit reporting and TFN complaints) and suggested that the Commissioner's powers to conduct investigations should be consistent regardless of the subject of the complaint.[157]

45.100 The OPC also commented on two restrictions placed on the personal information and documents that can be furnished or produced to the Commissioner during the investigation of a privacy complaint. Section 69 of the Act prevents people giving the Commissioner information generated for the purposes of taxation law or a law relating to census or statistics, unless it relates to an individual who has made a complaint. Secondly, it sets out 'very broad restrictions on the provision of information about an individual other than the complainant to the Commissioner', requiring that such information can only be provided with the individual's consent.[158] As the OPC noted, this provision overrides the Commissioner's powers to require information to assist an investigation (such as in s 44 of the *Privacy Act*).

45.101 While the OPC supported the first restriction, recognising the sensitive nature of information held by the ATO and the Australian Bureau of Statistics, it expressed concern about the second restriction:

> If applied rigorously this provision would make the complaint handling process very onerous both for organisations and agencies who are respondents to complaints under s 36 of the Act. For example, a description of an incident leading to a privacy complaint may be less meaningful or less convincing without naming third parties including employees. The lack of such information may make it difficult for the Commissioner to investigate. The process of obtaining consent may be difficult or costly.

45.102 The OPC observed that the rationale for the provision is unclear and 'appears to depart from the framework that would ordinarily be applied to a regulatory body'. The OPC suggested that the section be reframed to target more clearly the circumstances when third party consent would be required to furnish or produce information to the Commissioner.[159]

---

156 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
157 Ibid.
158 Ibid.
159 Ibid.

ALRC's view

45.103 In relation to compulsory conferences, the Explanatory Memorandum for the Privacy Bill 1988 (Cth) made it clear that ss 46 and 47 were intended to empower the Commissioner to 'direct persons to attend a compulsory conference in order to attempt a settlement of a complaint'.[160] The term 'compulsory conference' is only used in the section headings for ss 46 and 47. As the heading to a section of an Act is not taken to be part of the Act, the ALRC does not believe it is necessary for the word conciliation to be included in the section heading.[161] The OPC could clarify, however, the role of conferences in the conciliation process in the document setting out its complaint-handling policies and procedures.[162]

45.104 In the ALRC's view, the power to compel parties to attend a compulsory conference should extend to where the complaint is an NPP complaint, or a code complaint accepted under s 40(1B). Conciliation conferences are an important part of the conciliation process, and the Commissioner's powers to resolve complaints should be consistent across all types of complaints.

45.105 In relation to the OPC's concerns about s 69 of the *Privacy Act*, the ALRC's view is that the restrictions in s 69(1)–(2) on the Commissioner's ability to collect third party information in the process of investigating a complaint should be removed. These restrictions may fetter the ability of the Commissioner to resolve complaints efficiently and effectively, and are inconsistent with provisions applying to other regulators.[163] The ALRC also notes that the OPC is subject to secrecy provisions in s 96 of the *Privacy Act*, which make it an offence for the Commissioner or a member of his or her staff (present and past) to disclose, use or make a record of information acquired about a person in the performance of that role, other than to do something permitted or required by the *Privacy Act*.[164] These provisions provide protection for any information collected in an investigation.

45.106 In relation to the hearing requirements before a determination is made, the ALRC proposes that the *Privacy Act* should be amended to give the Commissioner flexibility to make determinations 'on the papers' in certain circumstances. The ALRC recognises that there may be situations where a determination could be made fairly and efficiently without parties appearing before the Commissioner to make oral

---

160 Explanatory Memorandum, Privacy Bill 1988 (Cth). This interpretation of compulsory conferences is also consistent with *Human Rights and Equal Opportunity Act 1986* (Cth) ss 46PJ(1), s 46PF(1).

161 See *Acts Interpretation Act 1901* (Cth) s 13(3).

162 See Proposal 45–8.

163 There is no equivalent provision in the *Human Rights and Equal Opportunity Act 1986* (Cth) or other state or territory privacy legislation.

164 *Privacy Act 1988* (Cth) s 96(1), (3). The offence is punishable by a penalty of $5,000 or imprisonment for 1 year, or both. Note that the OPC released its privacy policy (which sets out its personal information handling practices) in August 2006: Office of the Privacy Commissioner, *Privacy Policy* (2006).

submissions. The ALRC also recognises that the proposal that complainants and respondents be given the right, in certain circumstances, to require that a complaint be resolved by a determination would, if implemented, give rise to a consequent right for the complainant or respondent to appear before the Commissioner before a determination is made. The combination of the proposal and the current provision could increase the number of hearings held by the Commissioner, which may have significant resource implications. There is merit, therefore, in giving the Commissioner greater flexibility to make determinations on the papers.

45.107 There are several options to allow for determinations on the papers. The first is to remove the automatic right to appear before the Commissioner and instead give the Commissioner the discretion to provide a party with an opportunity to appear before him or her where the Commissioner considers that the circumstances require it, and in all other circumstances to make a determination based on written submissions. The second option is retain the current right to appear before the Commissioner to make oral or written submissions, but to provide explicitly that a hearing can be conducted on the basis of written submissions only where the parties agree. This is the approach taken in the *Social Security (Administration) Act*. This would allow for the entire hearing to be conducted on the papers where the parties consent.

45.108 In the ALRC's view, the second approach is preferable. The existing right to appear before the Commissioner should be retained but the Act should empower the Commissioner to make a determination on the basis of written submissions where the Commissioner considers that the determination could be made fairly in the absence of the parties and the parties consent to the determination being made without an oral hearing.

Proposal 45–11 Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference.

Proposal 45–12 Section 69(1) and (2) of the *Privacy Act* should be deleted, which would allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.

Proposal 45–13 The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if:

(a) the Privacy Commissioner considers that the matter could be determined fairly on the basis of written submissions by the parties; and

(b) the complainant and respondent consent to the matter being determined without oral submissions.

46. Enforcing the *Privacy Act*

Contents

Introduction 1275
Enforcing own motion investigations 1276
Background 1276
Remedies following own motion investigations 1276
Submissions and consultations 1277
ALRC's view 1278
Enforcing a determination 1279
Enforcement of determinations against organisations 1279
Enforcement of determinations against agencies 1279
Submissions and consultations 1280
ALRC's view 1280
Reports by the Commissioner 1281
Injunctions 1281
Background 1281
Submissions and consultations 1282
ALRC's view 1283
Other enforcement mechanisms following non-compliance 1283
Enforcement pyramid 1283
Submissions and consultations 1284
ALRC's view 1289

Introduction

46.1 The Office of the Privacy Commissioner (OPC) is responsible for enforcing compliance with the *Privacy Act 1988* (Cth). This involves investigating instances of non-compliance by agencies and organisations and prescribing remedies to redress non-compliance. While Chapter 45 examines the Privacy Commissioner's powers to investigate and resolve privacy complaints, this chapter considers the Commissioner's powers to investigate an act or practice on his or her own motion. It also considers the Commissioner's power to enforce complaint determinations, report on certain activities and apply for injunctions. Lastly, the chapter discusses other enforcement mechanisms that could be introduced into the Act.

Enforcing own motion investigations

Background

46.2 In addition to the Commissioner's power to investigate an act or practice when a complaint has been made, the Commissioner can also investigate an act or practice on his or her own motion where the Commissioner considers it desirable that the act or practice be investigated.[1] Own motion investigations are used by the OPC where it becomes aware of matters that may involve interferences with privacy through media reports, tip-offs, and notification of breaches by agencies or organisations.[2]

Remedies following own motion investigations

46.3 The Commissioner can report to the Minister on own motion investigations against agencies, file number recipients, credit reporting agencies or credit providers. Section 30 of the Act provides that, where the Commissioner has investigated an act or practice without a complaint having been made under s 36, the Commissioner may report to the Minister about the act or practice investigated and must report where the:

- Minister directs the Commissioner to do so; or

- Commissioner thinks the act or practice investigated is an interference with an individual's privacy and the Commissioner has not considered it appropriate to endeavour to settle the matter, or has tried to settle the matter without success.[3]

46.4 Section 30(6) of the Act specifies that these reporting obligations do not apply to a complaint made under s 36 in relation to an act or practice of an organisation or a complaint accepted under s 40(1B). The purpose of this subsection was said to be 'to clarify that there is no requirement to report to the Minister following investigations conducted by the Privacy Commissioner into the acts or practices of organisations'.[4]

46.5 The OPC stated in its Annual Report for 2005–06 that, in the majority of cases it investigated and found allegations to be substantiated following an own motion investigation, the respondent dealt with the issues of concern either on its own initiative or following the OPC's suggestions. The types of action taken included advice to people affected, apologies, retrieval and disposal of records, and changes in practice and procedures.[5]

---

1 *Privacy Act 1988* (Cth) s 40.

2 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), [3.4.1]. The Annual Report provides examples of situations investigated by the OPC on its own motion.

3 *Privacy Act 1988* (Cth) s 30(1). Currently, the relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2.

4 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 107.

5 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), [3.4.2].

46.6 The inability of the Commissioner to enforce remedies following an own motion investigation was commented on by stakeholders in the OPC's review of the private sector provisions of the *Privacy Act* (OPC Review) and the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry). In the former, stakeholders submitted that a wider power of enforcement should be conferred on the Commissioner. It was suggested that the Commissioner should 'be able to enforce any directions given in relation to findings after an own motion investigation', ensuring that 'light handed' measures taken by the Commissioner have the 'weight of possible further action attached to them'.[6]

46.7 In the OPC Review, the OPC acknowledged that it had 'experienced some difficulties' in dealing with potential privacy breaches where there was no individual complainant and where the respondent was not cooperative.[7] It recommended that the Australian Government consider amending the *Privacy Act* to 'provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the National Privacy Principles' (NPPs).[8] The Australian Government agreed with this recommendation.[9]

Submissions and consultations

46.8 Several stakeholders commented on the OPC's own motion investigation powers. The Consumer Credit Legal Centre (NSW) (CCLC) was supportive of the Commissioner's power to conduct own motion investigations as a means of addressing systemic issues raised by consumer representative groups and other third parties. It expressed disappointment, however, that these investigations do not occur as often as the CCLC felt was necessary.[10]

46.9 Several stakeholders reiterated the need for the Commissioner to have the power to enforce remedies following own motion investigations where the Commissioner finds a breach of the privacy principles.[11] The OPC supported the introduction of

---

6 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 145. See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 146.

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 155.

8 Ibid, rec 44. See also Ibid, 157.

9 Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006), [Item 44].

10 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

11 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

coercive orders as an enforceable remedy following an own motion investigation.[12] Other stakeholders submitted that the Commissioner should be given power to make and enforce determinations as a result of an own motion investigation and that such investigations should be the subject of public notice by the Commissioner.[13] It was also suggested that procedures be developed for appropriate intervention by interested parties, such as non-government organisations.[14]

ALRC's view

46.10 Own motion investigations provide a valuable tool for the Commissioner to investigate allegations of non-compliance that come to light via means other than a complaint being lodged. In order to make these investigations effective as a compliance tool, however, it is important that the Commissioner have adequate means to enforce remedies where he or she finds a breach of the NPPs, the Information Privacy Principles (IPPs) or other provisions in the *Privacy Act*.

46.11 Accordingly, the ALRC proposes that the *Privacy Act* be amended to allow the Commissioner to issue a notice to comply following an own motion investigation. The Commissioner should be empowered to determine in the notice that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual. Consistently with the ALRC's proposal in relation to determinations,[15] the Commissioner should also be empowered to prescribe in the notice that the agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the Act.[16]

46.12 As with determinations, the notice will be enforceable by proceedings in the Federal Court or Federal Magistrates Court. Unlike in the case of determinations, the ALRC does not propose that there be merits review of a notice to comply issued by the Commissioner. If the respondent in a notice to comply contests the Commissioner's findings or the actions prescribed in the notice, the respondent could choose not to comply with the notice and wait for the Commissioner to enforce it in the Federal Court by way of a hearing de novo.

Proposal 46–1 The *Privacy Act* should be amended to empower the Privacy Commissioner to:

12 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
13 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.
14 Ibid.
15 See Proposal 45–7.
16 The proposed wording for this power is based on the compliance notice model used in other privacy legislation: see *Information Privacy Act 2000* (Vic) s 44; *Health Records Act 2001* (Vic) s 66; *Information Act 2002* (NT) s 82.

(a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;

(b) prescribe in the notice that an agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*; and

(c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.

Enforcing a determination

46.13 The *Privacy Act* contains provisions for the enforcement of determinations made under s 52. These mechanisms are different depending on whether the respondent is an agency or organisation.

Enforcement of determinations against organisations

46.14 The respondent to a determination under s 52 or an approved privacy code must not repeat or continue conduct covered by a declaration and must perform the act or course of conduct covered by the declaration.[17] These obligations are enforceable in the Federal Court or the Federal Magistrates Court in proceedings commenced by the complainant, the Commissioner, or an adjudicator for the approved privacy code under which the determination was made.[18] If satisfied that the respondent has engaged in conduct that constitutes an interference with the privacy of the complainant, the court 'may make such orders (including a declaration of right) as it thinks fit'.[19] The court is to deal with the question of whether the respondent has engaged in conduct that constitutes an interference with privacy by way of a hearing de novo.[20]

Enforcement of determinations against agencies

46.15 As with organisations, an agency must not repeat or continue conduct covered by a declaration and must perform the act or course of conduct covered by the declaration.[21] Where the respondent to a determination is the principal executive of an agency, he or she is responsible for ensuring that the determination is brought to the

17 *Privacy Act 1988* (Cth) s 55. Section 52 of the *Privacy Act* sets out the declarations the Privacy Commissioner can make in a determination.
18 Ibid s 55A(1).
19 Ibid s 55A(2).
20 Ibid s 55A(5).
21 Ibid s 58.

attention of the relevant members, officers and employees of the agency and that those people desist from or perform conduct covered by the declaration.[22]

46.16 Unlike enforcement of determinations against organisations, where a determination against an agency or principal executive includes a declaration for compensation or reimbursement for expenses, the *Privacy Act* provides that the complainant is entitled to be paid the amount specified. The amount is recoverable either as a debt due to the complainant by the agency or the Commonwealth.[23] If an agency or the principal executive of an agency fails to comply with obligations in relation to a declaration, the Commissioner or complainant can apply to the Federal Court or Federal Magistrates Court for an order directing the agency or principal executive to comply.[24] In contrast to the provisions for organisations, the court does not have to assess, by way of a hearing de novo, whether the agency engaged in conduct that constituted an interference with privacy. Rather, on application under the Act, the court may make 'such other orders as it thinks fit with a view to securing compliance by the respondent'.[25]

Submissions and consultations

46.17 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* provisions for enforcing determinations are adequate and administered effectively.[26] The Australian Privacy Foundation described the enforcement as 'unfortunate' in that complainants and the Commissioner have to go through a hearing de novo to enforce a determination if an agency or organisation fails to comply with its terms.[27]

ALRC's view

46.18 Given the constitutional restrictions on the Commissioner exercising judicial power,[28] the ALRC does not propose any amendments to the enforcement provisions. The ALRC notes, however, that its proposal that the *Privacy Act* should be amended to provide for a complainant or respondent to seek merits review of determinations made by the Commissioner under s 52 may provide an alternative, and less costly, 'enforcement' mechanism for complainants than is currently provided in the Act.[29]

---

22 Ibid s 59.
23 Ibid s 60. This provision does not apply to organisations because of the limitations on Commonwealth judicial power.
24 Ibid s 62.
25 Ibid s 62(4). See also s 61(5) regarding timing of the application.
26 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–17.
27 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
28 See the discussion in Ch 45.
29 See Proposal 45–7. This was suggested by the Office of the NSW Privacy Commissioner: Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007.

Reports by the Commissioner

46.19 The Commissioner has powers to report on the exercise of some of his or her functions. In addition to the reporting obligations following certain own motion investigations discussed above, where the Commissioner has monitored an activity or conducted an audit in the performance of the functions in ss 27, 28 and 28A of the *Privacy Act*, the Commissioner may report to the Minister about the activity or audit, and must report if directed to do so by the Minister.[30] The Commissioner can give a further report to the Minister where the Commissioner believes it is in the public interest to do so, and the Minister must lay the report before each House of Parliament within 15 sitting days.[31]

46.20 There is no express power or obligation to report investigations of complaints and the *Privacy Act* does not explicitly envisage the Commissioner reporting directly to Parliament.[32] The ability to report on the results of audits, however, provides the Commissioner with another kind of 'enforcement' mechanism, as such reporting can involve a measure of publicity and sanction.

Injunctions

Background

46.21 The *Privacy Act* contains detailed provisions regarding the granting of injunctions. Section 98 provides that following an application from the Commissioner or another person, the Federal Court or Federal Magistrates Court can grant an injunction restraining a person from engaging in conduct that would constitute a contravention of the *Privacy Act* and, if the court thinks it desirable to do so, requiring a person to do any act or thing.[33] An injunction may be granted if it appears to the court that it is likely the person will engage in the relevant conduct if the injunction is not granted, whether or not the person has previously engaged in conduct of that kind, and whether or not there is an imminent danger of substantial damage to any person if the person engages in the relevant conduct.[34] Where the Commissioner applies for an injunction under s 98, the court will not require the Commissioner or any other person to give an undertaking as to damages.[35]

---

30 *Privacy Act 1988* (Cth) s 32. The relevant Minister is currently the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], pt 2. Certain matters may be excluded from reports—see *Privacy Act 1988* (Cth) s 33.

31 *Privacy Act 1988* (Cth) ss 30(4)–(5), 31(4)–(5), 32(2)–(3).

32 See Ibid s 30(6). See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.38]; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

33 *Privacy Act 1988* (Cth) s 98(1)–(2).

34 Ibid s 98(5)(b). See also s 98(6).

35 Ibid s 98(7).

46.22 Two features of the injunctions power are significant. First, it does not only concern enforcement of determinations.[36] It is a freestanding provision that deals with any contravention of the *Privacy Act*. Secondly, the 'standing' requirement is relatively easy to satisfy—the application may be made by the Commissioner 'or any other person'.[37]

46.23 There appear to be few cases in which an injunction has been granted to restrain contravention of the *Privacy Act*, though the remedy is potentially of general application and utility.[38] The OPC has stated that the Commissioner would seek an injunction only 'when other more informal means have failed to yield a satisfactory outcome'.[39]

Submissions and consultations

46.24 In IP 31, the ALRC asked whether the *Privacy Act* provisions for obtaining injunctions are adequate and effective.[40] The OPC expressed concern about the breadth of the standing provision in s 98. The OPC suggested that 'it could allow a party with no interest in the privacy of the individuals in question to seek an injunction that may, as a consequence, impact on how an agency or organisation interacts with that individual'.[41] The OPC recommended that s 98 be amended to include a more rigorous test for standing. In contrast, another stakeholder described the ability of non-government organisations to seek injunctions, because of the provision for open standing, as a 'theoretically valuable means by which contesting interpretations of principles could be resolved'.[42]

46.25 The Australian Privacy Foundation also submitted that the injunction power is valuable and that the Commissioner should make greater use of the power, 'both during complaint investigations and as a pro-active tool where interferences with privacy are brought to attention in other ways'.[43] The Queensland Council for Civil Liberties saw no reason to alter the position in relation to obtaining injunctions.[44]

---

36 See N Witzleb, 'Federal Court Strengthens Privacy Enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45, 45.

37 This is similar to the position in the *Trade Practices Act 1974* (Cth) s 80. See also *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145, [40], [55].

38 See *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145.

39 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 3.

40 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–19.

41 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

42 G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007. The ability to seek an injunction was said to be 'inherently valuable'.

43 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

44 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007.

ALRC's view

46.26 The ALRC does not propose any reform to the injunction provisions. The power is comparable to provisions for statutory injunctions under the *Trade Practice Act 1974* (Cth) (TPA) and the *Corporations Act 2001* (Cth).[45] While the provisions have not been utilised often, the power itself is appropriate. The ALRC also recognises the value in providing for open standing in this area, because it allows consumer and privacy organisations to initiate proceedings under the section.[46] As noted by Dr Norman Witzleb:

> This may prove of particular use where large organisations introduce services which have the potential of presenting privacy threats on a massive scale—such as, for example, the recently introduced 'g-mail' service by *Google*, which prompted substantial criticism from privacy and consumer groups worldwide.[47]

46.27 Greater use could be made of the injunctions power if the ALRC's proposal that the *Privacy Act* be amended to empower the Commissioner to direct an agency or organisation to prepare a privacy impact assessment is implemented.[48] If a project or development raised serious privacy concerns and the Commissioner believed it would, if implemented, interfere with the privacy of individuals, the Commissioner could seek an injunction from the Federal Court or Federal Magistrates Court to stop the project.[49]

Other enforcement mechanisms following non-compliance

Enforcement pyramid

46.28 As discussed in Chapter 42, Professors Ian Ayres and John Braithwaite have suggested that the ideal regulatory approach to enforcing compliance with regulation is through the adoption of an explicit 'enforcement pyramid'. Under such a model, regulators use coercive sanctions only when less interventionist measures have failed to produce compliance.[50] Breaches of increasing seriousness are dealt with by sanctions of increasing severity, with the most serious or 'ultimate sanctions' generally held in reserve as a threat.

---

45 See *Trade Practices Act 1974* (Cth) s 80; *Corporations Act 2001* (Cth) s 1324.

46 See also Australian Law Reform Commission, *Beyond the Door-keeper: Standing to Sue for Public Remedies*, ALRC 78 (1996).

47 N Witzleb, 'Federal Court Strengthens Privacy Enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45, 49.

48 See Proposal 44–4.

49 See *Privacy Act 1988* (Cth) s 98.

50 The model was first put forward in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985) and was further discussed in B Fisse and J Braithwaite, *Corporations, Crime and Accountability* (1993); C Dellit and B Fisse, 'Civil and Criminal Liability Under Australian Securities Regulation; The Possibility of Strategic Enforcement' in G Walker and B Fisse (eds), *Securities Regulation in Australia and New Zealand* (1994), 570.

46.29 There is great value in adopting the enforcement pyramid structure in the *Privacy Act*, as discussed further in Chapter 42. In some respects, the *Privacy Act* already adopts a pyramid-type structure for enforcing compliance. The approach relies initially on encouraging compliance, with determinations (and enforcement in the courts) and injunctions held in reserve. While there is some degree of escalation involved in these remedies, there are no civil penalties for serious contraventions of the Act, except some limited criminal penalties attached to credit reporting, and tax file number, offences.[51]

Submissions and consultations

46.30 In IP 31, the ALRC asked whether the range of remedies available to enforce rights and obligations created by the *Privacy Act* required expansion. Further remedies suggested by the ALRC include administrative penalties, enforceable undertakings or other coercive orders, remedies in the nature of damages, infringement notices, civil penalties and criminal sanctions.[52]

46.31 The ALRC received mixed responses from stakeholders about the need for further enforcement mechanisms. The Australian Health Insurance Association suggested that harsher penalties under the Act are unnecessary as it has not been shown that the lack of 'teeth' in privacy legislation has reduced compliance with privacy laws.[53] In contrast, the Australian Privacy Foundation submitted that a wider range of remedies and sanctions is desirable.[54]

46.32 Some stakeholders also commented on the resources needed to pursue an expanded range of remedies. The Fundraising Institute–Australia observed that, for the Commissioner to administer the complete range of penalties identified in IP 31, significant additional resources would be required.[55] While recognising the resource implications of additional remedies, the CCLC observed that

> stronger enforcement mechanisms, including through civil pecuniary penalties, present the OPC with a more long-term cost-effective way of functioning. Forcing businesses and industry to be accountable by imposing greater deterrents should result in less cases and investigations by the OPC.[56]

46.33 The ALRC also received comments on some of the particular remedies described by the ALRC in IP 31, which are discussed below.

---

51 The ALRC proposes the repeal of these credit reporting offences: see Proposal 55–8.

52 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 6–22. The remedies are discussed in more detail at [6.180]–[6.205].

53 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

54 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

55 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007. See also Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

56 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

Administrative penalties and infringement notices

46.34 Several stakeholders commented on the use of administrative penalties and infringement notices. Administrative penalties are automatic, non-discretionary monetary penalties that are imposed without intervention by a court or tribunal.[57] Infringement notices are administrative methods of dealing with certain breaches of the law. When such a breach is committed, the regulator 'may prosecute or take civil penalty proceedings, or may issue an infringement notice offering the offending party the chance to discharge or expiate the breach through payment of a specified amount'.[58] The ALRC has previously expressed the view that infringement notice schemes are 'constitutionally valid where they do not involve a regulator assessing a penalty after a hearing of any description, but merely applying the law that determines the breach, together with a statement of the amount that the notice invites the alleged offender to pay'.[59] Both the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) set up systems of infringement notices for contraventions of civil penalty provisions, as an alternative to the regulator instituting proceedings in the Federal Court.[60]

46.35 The OPC considered that administrative penalties or infringement notices would usefully address the compliance issues that arise in the *Privacy Act*. The OPC suggested that a non-discretionary fine would not be suitable in a complaints framework, where the OPC must assess different versions of an event and establish whether an exception to the general rule applies in the particular circumstances. Similarly, the OPC queried whether infringement notices would be appropriate in individual complaints that are frequently contested. The OPC considered it unlikely that there would be many circumstances in which an infringement notice could lawfully be issued prior to an investigation having been undertaken.[61]

46.36 In contrast, the Australian Privacy Foundation suggested that the experience of other jurisdictions suggests that administrative penalties and infringement notices can be particularly effective, noting that both the *Spam Act* and the *Do Not Call Register Act* include such provisions.[62] AAMI also noted that infringement notices could be used as a first step in a pyramid approach to penalties.[63] The CCLC submitted that administrative penalties have 'great potential for ensuring compliance' because the

---

57 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.64], [2.70].
58 Ibid, [2.67].
59 Ibid, [2.130].
60 See *Spam Act 2003* (Cth) sch 3; *Do Not Call Register Act 2006* (Cth) sch 3.
61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
62 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
63 AAMI, *Submission PR 147,* 29 January 2007.

non-discretionary nature of the penalty could 'posit accuracy and privacy protection as norms and just part of "good practice"'.[64]

Coercive orders

46.37 The ALRC noted in IP 31 that enforceable undertakings may be a possible remedy for breaches of the *Privacy Act*. The ALRC has previously described an enforceable undertaking as 'a promise enforceable in court'. A breach of the undertaking is not contempt of court but, once the court has ordered the person to comply, a breach of that order is contempt.[65]

46.38 Another type of coercive order is the compliance notice model used in other privacy legislation. For example, the *Information Act 2002* (NT) gives the Information Commissioner the power to serve a compliance notice on an organisation if it appears that the organisation has contravened a privacy principle, and the contravention is serious or flagrant or contraventions of that kind have occurred on three occasions within the previous two years. The notice requires the organisation to take specified action to ensure it complies with the privacy principles in the future. Failure to comply with the notice is an offence with a significant monetary penalty.[66]

46.39 The Office of the Information Commissioner Northern Territory described this compliance notice scheme as 'an effective compliance measure that could be used in respect of serious breaches by agencies or organisations'.[67] The OPC suggested that the compliance notice model was more appropriate in the privacy context than an enforceable undertaking. It noted that, in the trade practices context, enforceable undertakings operate as an alternative to litigation. As the Commissioner cannot prosecute organisations for breaches of the *Privacy Act*, the same incentive for organisations to commit to enforceable undertakings is not present.[68] The CCLC observed that, in its experience, enforceable undertakings are not very useful, 'especially as one must ultimately rely on a court to ensure results'.[69]

46.40 In contrast, AAMI found that the Australian Securities and Investments Commission uses this remedy effectively and suggested that it could be used in the privacy context in circumstances where an organisation continually breaches the Act, despite formal and repeated warnings from the regulator.[70] The Law Council of

---

64 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
65 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.159].
66 *Information Act 2002* (NT) s 82.
67 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
68 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
69 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
70 AAMI, *Submission PR 147,* 29 January 2007.

Australia suggested that enforceable undertakings would give the Commissioner the ability to enforce a certain level of compliance without needing to turn to the courts.[71]

46.41 As discussed above, the ALRC has adopted a similar mechanism to the compliance notice in Proposal 46–1. Under the ALRC's proposal, however, a compliance notice could be issued only where the Commissioner finds an interference with privacy following an own motion investigation. Where the Commissioner finds an interference with privacy following a complaint investigation—which is the only other way the Commissioner can investigate a possible interference with privacy under the Act—the ALRC has proposed that the Commissioner be empowered to make orders in a determination that an agency or organisation must take specified action within a specified period for the purpose of bringing itself into compliance with the *Privacy Act*. This power is analogous to the proposed compliance notice and can be understood as a type of coercive order.

Remedies in the nature of damages

46.42 There is currently no provision for direct civil action by individuals against agencies or organisations that breach the *Privacy Act*. In contrast, the TPA provides that a person who suffers loss or damage by conduct of any person that was done in contravention of specific parts of the TPA may recover the amount of the loss or damage by action against that other person or against any person involved in the contravention.[72]

46.43 Some stakeholders supported providing individuals with an avenue for seeking damages via the development of a tort of privacy.[73] Beyond this, the OPC favoured the conciliation model as the primary complaint-handling model under the Act, including where an individual is seeking compensation. The OPC noted the high costs involved in pursuing a matter through the courts and the low level of compensation awarded in the resolution of privacy complaints. The OPC also observed that individuals could pursue compensation through the federal courts where an organisation does not comply with a determination.[74]

---

71 Law Council of Australia, *Submission PR 177,* 8 February 2007. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005 as affirmed in Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

72 *Trade Practices Act 1974* (Cth) s 82.

73 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Joint submission by Industry Based Alternative Dispute Resolution Schemes, *Submission PR 93,* 15 January 2007. The development of a statutory cause of action for invasion of privacy is discussed further in Ch 5.

74 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

Publicity

46.44 Publicity can be a formal, legislated sanction or operate to create a negative perception of an agency or organisation by virtue of the imposition of another penalty.[75] The OPC has outlined that it will only use publicity in rare circumstances, given the serious 'commercial consequences' that can flow from making public the circumstances of a particular complaint or investigation.[76] The OPC has issued media statements outlining the actions taken in respect of particular organisations and agencies.[77]

46.45 The CCLC suggested that adverse publicity 'has a great potential as a weapon to ensure an organisation's compliance as this can impact on investment as well as potential for future customers or clients'.[78] The CCLC described it as a 'drastic measure', and suggested that its use could be limited to more extreme circumstances and for recurrent offenders. Another stakeholder stated that using publicity as an enforcement response was contrary to the concept of privacy and the spirit of the *Privacy Act*.[79]

Civil pecuniary penalties

46.46 Civil pecuniary penalties are essentially punitive—although their chief aim is often said to be deterrence—and they are payable whether or not harm was actually caused by the unlawful action.[80] A number of stakeholders in the OPC Review submitted that there should be some level of civil penalty resulting from a contravention of the *Privacy Act*.[81] One stakeholder stated that it is hard to convince some company boards to comply with privacy laws when no schedule of penalties is attached to non-compliance with the NPPs.[82] This view was also expressed in a number of consultations.

46.47 In its submission, the OPC acknowledged the comments made by stakeholders in the OPC Review, but considered that there are 'few circumstances where the introduction of civil penalties would be appropriate'.[83] In line with an enforcement

---

75 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.138].

76 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 3.

77 See, for example Office of the Federal Privacy Commissioner, 'Deputy Federal Privacy Commissioner Concludes Harts Investigation' (Press Release, 12 February 2001); Office of the Federal Privacy Commissioner, 'Federal Privacy Commissioner Negotiates Change in the Debt Collection Practices of Alliance Factoring' (Press Release, 4 July 2003).

78 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.

79 I Turnbull, *Submission PR 82,* 12 January 2007.

80 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.107].

81 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 132–133.

82 Ibid, 133. Note it is unclear whether 'penalties' relates to criminal or civil penalties (or both).

83 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

pyramid approach to compliance under the *Privacy Act*, however, civil penalties could be considered as a sanction for failure to comply with a compliance notice following an own motion investigation.[84] The OPC also suggested that civil penalties could apply to failure to report a data breach, if such a requirement were introduced into the Act.[85]

46.48 The CCLC submitted that imposing civil penalties, regardless of whether harm has been caused by the breach, 'is another effective measure for compliance'. The CCLC submitted that ss 16 and 16A of the Act should be nominated as civil penalty provisions, and suggested that any money generated by the penalty could be directed towards a privacy fund dedicated to enforcement.[86] Another stakeholder observed that the Act is not amenable to civil penalties because of the 'random extent of the exceptions and exemptions'. If the exemptions and exceptions were removed or limited, however, the Act could be amended to provide civil penalties enforceable by the OPC 'upon request by aggrieved individuals'.[87]

Criminal penalties

46.49 The *Privacy Act* already contains some criminal offences. For instance, furnishing information knowing that it is false or misleading in a material particular is an offence carrying a penalty of $2,000 or 12 months' imprisonment, or both.[88] There are also offences in the credit reporting provisions. For example, a credit reporting agency that intentionally contravenes s 18K(1) or s 18K(2)—which set limits on the disclosure of personal information by credit reporting agencies—is guilty of an offence punishable, on conviction, by a fine not exceeding $150,000.[89]

46.50 There was no support for introducing further criminal penalties into the *Privacy Act*, such as for a reckless, intentionally dishonest or flagrant contravention. The OPC considered that a cautious approach should be taken to the inclusion of further criminal sanctions, and noted that 'as privacy is unlikely to be a high policing priority, a significant increase in criminal sanctions may impede rather than facilitate better privacy protection and privacy complaint outcomes'.[90]

ALRC's view

46.51 The framework of compliance-oriented regulation underpinning the *Privacy Act* should be considered when examining whether there should be further penalties added to the Act. As discussed in Chapter 42, a compliance-oriented approach to

---

84 A similar model was proposed in Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.91].
85 This is discussed further in Ch 47.
86 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 160,* 31 January 2007.
87 I Turnbull, *Submission PR 82,* 12 January 2007.
88 *Privacy Act 1988* (Cth) s 65(3).
89 Ibid s 18K(4). The ALRC proposes the repeal of these provisions: see Proposal 55–8.
90 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

enforcement, which includes a focus on fostering compliance in the first instance, requires the presence of punitive sanctions to be effective. This is because 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.[91] The existence of a strong penalty can, by itself, act as an incentive for compliance, as long as the regulated entity knows that the regulator will impose the penalty where appropriate.

46.52 Determinations are regarded by some as a 'strong' penalty, because they can involve a public declaration of breach and thereby contain an element of informal, negative publicity.[92] The ALRC notes, however, that according to the OPC's new determination policy, determinations are not necessarily going to be limited to the most serious cases, 'nor will determinations issued by the Commissioner necessarily be punitive'.[93] This approach by the OPC is consistent with the ALRC's proposal to increase the number of determinations issued, by giving complainants and respondents the right to require the Commissioner to issue a determination in certain circumstances.[94]

46.53 Although the significance of determinations should not be underestimated, the ALRC believes there is a need to strengthen the overall enforcement pyramid of the *Privacy Act*. Accordingly, it proposes that the Act should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual.[95] The Commissioner should be empowered to bring proceedings for pecuniary penalties in the Federal Court, similar to the approach taken with the Australian Competition and Consumer Commission (ACCC) under the TPA.[96]

46.54 Consistently with the ALRC's recommendation in *Principled Regulation* (ALRC 95), the ALRC proposes that the OPC develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty under the *Privacy Act* would be made.[97] It is likely that the OPC would only undertake civil penalty proceedings where the matter involves: an apparent blatant disregard of the law; a history of previous contraventions of the law; significant public detriment or

---

91 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529, 539. See also J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science.

92 Determinations are published, with the respondent's name, at Office of the Privacy Commissioner, *Complaint Case Notes, Summaries and Determinations* (2007) <www.privacy.gov.au/act/casenotes/index.html> at 1 August 2007.

93 Office of the Privacy Commissioner, 'Commissioner's Use of s 52 Determination Power' (2006) 1(1) *Privacy Matters* 2, 2.

94 See Proposal 45–5.

95 See also Proposal 55–8.

96 *Trade Practices Act 1974* (Cth) s 77.

97 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 10–1.

significant number of complaints; or the potential for action to have a worthwhile educative or deterrent effect.[98]

46.55 The ALRC does not propose that an administrative penalty or infringement notice scheme be included in the Act. The ALRC acknowledges the difficulties of using non-discretionary fines and infringement notices in the context of the principles-based regime of the *Privacy Act*. The ALRC also does not propose that enforceable undertakings be introduced in the Act. The ALRC's proposals to introduce compliance notices for own motion investigations and to expand the remedies available in a determination empower the Commissioner to make coercive orders and will provide additional methods to enforce the *Privacy Act*.

Proposal 46–2 The *Privacy Act* should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual. The Office of the Privacy Commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty is made.

98 These factors are similar to the enforcement priorities of the ACCC: see Australian Competition and Consumer Commissioner, *Section 87B of the Trade Practices Act: A Guideline on the Australian Competition and Consumer Commission's Use of Enforceable Undertakings* (1999), 2.

47. Data Breach Notification

Contents

Overview 1293
- Background 1293
- Current regulatory requirements 1294

Rationale for data breach notification 1294
- Identity theft 1294
- Lack of market incentives for notification 1296
- Provides incentives to secure data 1296
- Increasing number of data breaches 1297

Models of data breach notification laws 1297
- Background 1297
- Trigger for notification 1298
- Definition of 'personal information' in data breach notification laws 1300
- Exceptions 1301
- Responsibility to notify 1302
- Timing, method and content of notification 1303
- Penalties for failure to notify 1305

Submissions and consultations 1306
- General support 1306
- Opposing a data breach notification requirement 1306
- Triggers for reporting 1307

ALRC's view 1309
- Data abuse pyramid 1309
- Trigger for notification 1311
- Exceptions 1312
- 'Specified personal information' for the purposes of notification 1313
- Other matters 1314
- Penalties 1316

Overview

Background

47.1 Data breach notification is a topical issue in privacy regulation around the world. Data breach notification is, in essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information.

47.2 This chapter starts by considering the rationales given for data breach notification laws in the United States (US), which is at the forefront in the development of such laws. The chapter then considers some of the key elements of data breach notification laws in other jurisdictions, including the event that triggers the requirement to notify. Finally, the chapter sets out the ALRC's view on the justification for a data breach notification law and proposes that the *Privacy Act 1988* (Cth) be amended to include a new part on data breach notification.

Current regulatory requirements

47.3 The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the *Privacy Act* do not impose an obligation on agencies and organisations to notify individuals whose personal information has been compromised. The *Privacy Act* requires, however, that agencies and organisations take reasonable steps to maintain the security of the personal information they hold.[1]

47.4 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC asked whether the *Privacy Act* should be amended to require agencies or organisations to advise individuals of any misuse, loss or unauthorised access, modification or disclosure of personal information.[2] If the answer to this threshold question is 'yes', further issues arise about the nature and extent of such an obligation. Specifically, should the obligation extend to any unauthorised disclosure or only those disclosures that could lead to harm, such as identity theft?

Rationale for data breach notification

Identity theft

47.5 In the US, concerns about identity theft and identity fraud have been the main issues driving the development of data breach notification laws.[3] As discussed in Chapter 9, identity theft is a subset of the broad concept of 'identity crime' and is used to describe the illicit assumption of a pre-existing identity of a living or deceased person, or of an artificial legal entity such as a corporation.[4] A stolen identity can be used to commit 'identity fraud', which is where a fabricated, manipulated or stolen identity is used to gain a benefit or avoid an obligation. An example of identity fraud is using a stolen identity to make fraudulent purchases or steal money from the victim (known as 'account takeover').[5] Another example of identity fraud is where a criminal

---

1 *Privacy Act 1988* (Cth) s 14, IPP 4; sch 3, NPP 4. See also the proposed 'Data Security' principle in the Unified Privacy Principles set out at the beginning of this Discussion Paper.

2 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–35, 11–3(d).

3 See Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1. Ch 9 discusses identity theft—and the related concepts of 'identity crime' and 'identity fraud'—in more detail.

4 Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006), 15.

5 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 2.

uses personal information about an identity theft victim to open new accounts in the name of the victim (sometimes called 'true name fraud').[6]

47.6 With advances in technology, agencies and organisations are storing vast amounts of identifying information electronically.[7] Any breach of the secure storage of this information can result in the release of personal, identifying information of an individual. That personal information may be sufficient to allow an unauthorised person to assume the identity of the victim and use that illicit identity to open, for example, new accounts in the victim's name.

47.7 For these reasons, a security breach, resulting in unauthorised 'leaks' or acquisitions of information, is thought to contribute to the risk of identity theft, and the consequent risks of identity fraud.[8] By requiring notice to persons who may be affected adversely by a breach, data breach notification laws 'seek to provide such persons with a warning that their personal information has been compromised and an opportunity to take steps to protect themselves against the consequences of identity theft'.[9] As one commentator explains:

> Identity theft and identity fraud have emerged as serious crimes for consumers, citizens and business … Given the peculiar nature of this type of theft—namely, that it can be perpetrated by accessing information stored in places uncontrolled by the victim and in places of which the victim is often unaware—legislators have passed or are considering passing laws which require that the consumer be notified in the event of a data breach.[10]

47.8 Data breach notification laws are, therefore, based on the recognition that 'individuals need to know when their personal information has been put at risk in order to mitigate potential identity fraud damages'.[11]

---

6 See Ibid, 2.

7 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1.

8 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

9 T Smedinghoff, *Security Breach Notification—Adapting to the Regulatory Framework* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007, 1–2. See also M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 11; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1–2.

10 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 2.

11 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 2.

Lack of market incentives for notification

47.9 Some commentators suggest that the obligation to notify individuals of a data breach needs to be mandated legally because the market, by itself, may not provide sufficient incentives for organisations to take measures to notify individuals affected by the breach.[12] In particular, an organisation may not have an incentive to notify individuals affected by a security breach when the 'cost' of the notification exceeds the expected damage to the organisation.[13]

47.10 The cost of notification does not just include the actual cost involved in notifying every individual affected by a security breach, although that, by itself, can be very expensive. Notifying customers of a security breach also gives rise to a real potential for market damage to the organisation, including reputational damage, lost customers and lost future profits. Notification can also expose an organisation to civil penalties from regulators and costly private litigation proceedings by individuals affected. If the organisation has a high profile or the security breach is large, notification can also result in negative publicity in the media. In these circumstances, an organisation may avoid reporting a security breach if it is not legally required to do so, as the cost to the organisation of notifying individuals significantly outweighs the costs caused by the actual breach. For these reasons, therefore, it has been observed that, in the absence of a legal requirement to notify, market forces may 'undersupply notification'.[14]

Provides incentives to secure data

47.11 Given the reputational damage that can flow from having to disclose a security breach, it has been suggested that the existence of a data breach notification law provides commercial incentives for organisations to take adequate steps in the first place to secure data.[15] The purpose of the Delaware data breach notification legislation, for example, is to 'help ensure that personal information about Delaware residents is protected by encouraging data brokers to provide reasonable security for personal information'.[16] This is an important effect of data breach notification, particularly as organisations in the US may not be subject to express data security obligations such as those in the *Privacy Act*.[17]

---

12 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 11–12.

13 Ibid, 12.

14 Ibid, 13.

15 B Arnold, 'Losing It: Corporate Reporting on Data Theft' (2007) 3 *Privacy Law Bulletin* 101, 102. See also T Smedinghoff, *The New Law of Information Security: What Companies Need to Do Now* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 22.

16 *Delaware Code* , Synopsis. Similar comments are made in *Arkansas Code* § 4-110-102.

17 Some of the data breach notification laws, however, also require regulated entities to implement and maintain reasonable security procedures and practices: see, eg, *Arkansas Code* § 4-110-104.

Increasing number of data breaches

47.12 The rapid growth in data breach notification laws in the US in the past few years is said to be a direct response to a series of high profile, well-publicised data breaches.[18] One of the most notorious data breaches was the disclosure by ChoicePoint, a large identification and credential verification organisation in the US, of sensitive information it had collected on 145,000 individuals.

47.13 The Privacy Rights Clearinghouse maintains a Chronology of Data Breaches, which lists all breaches reported in the US that expose individuals to identity theft or breaches that qualify for disclosure under state laws. As at 18 July 2007, the total number of records containing sensitive personal information involved in security breaches was 150 million.[19] Security breaches are, therefore, a concern in the US community.

Models of data breach notification laws

Background

47.14 California was the first US state to require the reporting of data breaches involving personal information. The Californian law has been a model for legislation passed in over 30 US state legislatures and there are moves to implement a national notification standard concerning compromised data.[20] While many states adopt very similar provisions to the Californian law, some US states set a different test of when notification will be required.

47.15 While organisations are subject to differing data breach notification requirements depending on which state they operate in, all financial institutions in the US are subject to the data breach notification requirements set out in the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, issued by the US Department of Treasury and other agencies (US Interagency Guidance). The US Interagency Guidance interprets the requirements of the *Gramm-Leach-Bliley Act 1999* (US), which regulates all financial services institutions in the US, to develop and implement a response program 'to address unauthorized access to, or use of customer information that could result in substantial harm or inconvenience to a customer'.[21] The US Interagency Guidance only applies to

---

18 See Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 1–2. See also T Smedinghoff, *Security Breach Notification—Adapting to the Regulatory Framework* (2005) Baker & McKenzie <www.bakernet.com/ecommerce> at 31 July 2007, 1.

19 Privacy Rights Clearinghouse, *A Chronology of Data Breaches—Updated to 18 July 2007* <www.privacyrights.org/ar/ChronDataBreaches.htm> at 22 July 2007.

20 M Coyle, 'Industry, Government Fret Over Tactics for Fighting Data Theft', *National Law Journal* (online), 10 August 2006, <www.law.com/jlp/nlj/index.jsp>.

21 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer*

financial services institutions, and does not apply to other organisations or federal or state government agencies.

47.16 In Canada, only the province of Ontario requires notification after a security breach.[22] The Privacy Commissioners of Canada, British Colombia and Ontario have, however, issued a 'Breach Notification Assessment Tool' to assist organisations in determining what steps should be taken in the event of a privacy breach.

47.17 There have also been moves at the federal level in Canada to introduce a data breach notification law. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) issued in January 2007 a White Paper, *Approaches to Security Breach Notification*, which puts forward a model law for Canada. In addition, the review of the *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act), by the Canadian Government Standing Committee on Access to Information, Privacy and Ethics, considered the issue of breach notification. The Committee recommended that the PIPED Act be amended to include a breach notification provision requiring organisations to report certain defined breaches of personal information holdings to the Canadian Privacy Commissioner. The Canadian Privacy Commissioner would then determine whether or not affected individuals and others should be notified and, if so, in what manner.[23]

47.18 There are, therefore, a number of proposed or established models for data breach notification laws. These laws, however, adopt a variety of approaches on key areas such as the triggering event, exceptions to the notification requirement and responsibility to notify. The following section focuses on the key approaches taken in data breach notification laws in California and other US states, the US Interagency Guidance and the CIPPIC proposal in Canada.

Trigger for notification

47.19 In California, the event that triggers the obligation to provide notice is any 'breach of the security of the system', which is defined as the 'unauthorised acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency'.[24] A good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency does not constitute a breach of the security of the system, 'provided that the personal information is not used or subject to further unauthorised disclosure'.[25] This is said to

---

Information and Customer Notice (2005). See *Gramm-Leach-Bliley Act 1999* 15 USC §§ 6801–6809 (US).

22 See *Personal Health Information Protection Act 2004* (Ontario) s 12.

23 Canadian Government Standing Committee on Access to Information Privacy and Ethics, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)—Fourth Report* (2007), 45.

24 *California Civil Code* § 1798.29(a).

25 Ibid § 1798.29(d).

provide an exception to the general obligation to notify for 'harmless internal breaches'.[26]

47.20 The Californian triggering event of any 'unauthorised acquisition' of computerised data sets quite a low threshold for notification, as it requires notification even if the organisation considers it very unlikely that the personal information acquired could give rise to a risk of harm or identity theft. While this triggering event has been followed in a number of other US states,[27] some US states have adopted a higher threshold for notification. For example, the Indiana Code requires notification where there has been unauthorised acquisition of personal information 'if the database owner knows, should know, or should have known that the unauthorised acquisition constituting the breach has resulted in or could result in identity deception, identity theft or fraud affecting the Indiana resident'.[28] Other US states provide an exception to notification if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.[29]

47.21 In its approach to defining the triggering event, the US Interagency Guidance gives the relevant organisation greater discretion to decide whether notification is necessary. The US Interagency Guidance provides that when an institution becomes aware of an incident of unauthorised access to sensitive customer information, the institution should conduct a reasonable investigation to determine promptly the likelihood that the information has been, or will be, misused. If the institution determines that misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible.[30]

47.22 In its proposed model for Canada, the CIPPIC picked up on the Californian triggering event of 'acquisition or reasonable belief of acquisition by an unauthorised person'. The CIPPIC argued that this standard 'is higher than mere "access by an unauthorised person", but lower than standards that incorporate a "risk of identity fraud" element'.[31] The CIPPIC suggested that:

> The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created.[32]

---

26 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

27 See, eg, *Delaware Code* §§ 12B-101–12B-102; *New York State Code* § 899-aa(1).

28 *Indiana Code* § 24-4.9-3-1(1)(a). A similar approach is taken in *Ohio Revised Code* § 1347.12(B)(1).

29 See, eg, *Arkansas Code* § 4-110-105(d).

30 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

31 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 24.

32 Ibid, 25.

Definition of 'personal information' in data breach notification laws

47.23 The data breach notification laws in each state define the type of 'personal information' which, when leaked, may give rise to the obligation to notify. For the purpose of data breach notification, the definition of 'personal information' tends to focus more on the combination of certain pieces of personal information rather than providing a broad definition like that provided in the *Privacy Act*. References to 'personal information' in the context of data breach notification, therefore, are not meant to refer to personal information as defined in the *Privacy Act*.

47.24 The general approach adopted in a number of states, including California, is to define personal information as an individual's first name (or initial) and last name in combination with any of the following:

- social security number;
- driver's licence number or state identification card number; or
- account number, credit card number, debit card number in combination with any necessary security code, access code or password that would permit access to the account.[33]

47.25 Some US states include medical information in the definition of 'personal information'. For example, the Delaware code defines 'personal information' to include 'individually identifiable information, in electronic or physical form, regarding the Delaware resident's medical history or medical treatment or diagnosis by a health care professional'.[34]

47.26 The CIPPIC's proposed law for Canada defines 'designated personal information' in a similar manner as California, although it includes the combination of an address by itself (that is, without a name as well) with other sensitive information within the definition of 'designated personal information'. The CIPPIC justified this approach on the basis that 'it is relatively easy to obtain a person's name from an address, using phone books, online databases and search engines'.[35]

47.27 Under the Californian definition and a number of other US states, personal information does not include 'publicly available information that is lawfully made

---

33 *California Civil Code* § 1798.29(e). A similar definition is adopted in United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

34 *Delaware Code* § 12B-101(2). See also *Arkansas Code* § 4-110-103.

35 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

available to the general public from federal, state, or local government records'.[36] The US Interagency Guidance, however, outlines that it would be inappropriate to exclude publicly available information from the definition of sensitive customer information where the publicly available information is otherwise covered by the definition of customer information. For example, while a personal identifier, such as a name or address, may be publicly available, it is sensitive customer information when linked with particular non-public information such as a credit card account number.[37]

Exceptions

Encryption

47.28 Most states that have data breach notification laws, including California, do not require notification where the personal information that was the subject of the unauthorised acquisition was encrypted.[38] Some US states specify that the exception does not apply where the encryption key was also acquired.[39] The CIPPIC model also made an exception for encrypted data.[40]

47.29 In contrast, the US Interagency Guidelines rejected a blanket exclusion for encrypted data because 'there are many levels of encryption, some of which do not effectively protect customer information'.[41]

47.30 To address the differing standards of encryption and provide more guidance to organisations, some US states define encryption in the statute. For example, the Indiana Code provides that data are encrypted for the purposes of the data breach notification law if data:

> (1) have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or
>
> (2) are secured by another method that renders the data unreadable or unusable.[42]

---

36 *California Civil Code* § 1798.29(f). See also *New York State Code* § 899-44(1)(b); *Delaware Code* §§ 12B-101(2); *Ohio Revised Code* § 1347.12(A)(6).

37 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

38 *California Civil Code* § 1798.29(a).

39 See, eg, *New York State Code* § 899-44(1)(b); *Indiana Code* § 24-4.9-3-1(1)(a)(2).

40 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

41 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

42 *Indiana Code* § 24-4.9-2-5. See also *Ohio Revised Code* § 1347.12(A)(4).

47.31 Others US states give the organisation discretion to determine what constitutes valid encryption under the statute.[43] As this CIPPIC explains, this 'provides latitude to organisations in selecting encryption applications that suit them'.[44]

Redaction

47.32 Some US states also provide an exception to notification for data that is redacted. Redaction can refer to a variety of practices. In Indiana, redaction is defined as data that are altered or truncated so that not more than the last four digits of a driver's licence number, stated identification number, or account number, are accessible as part of personal information.[45] The CIPPIC proposal for a Canadian data breach notification law also proposes exceptions for 'information that is redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable by unauthorized persons'.[46]

Responsibility to notify

47.33 In all US states and in the US Interagency Guidance, the responsibility for deciding whether notification is required following a breach in the security of the system rests with the organisation itself.[47] The CIPPIC adopted a similar approach in its proposed model for Canada, providing that organisations should have the responsibility for determining whether the standard for breach notification is met.[48] The CIPPIC acknowledged that generally the affected organisation is in the best position to calculate the associated risks of a breach of its information security and should be entrusted with this determination.[49]

47.34 In all the proposed models considered by the ALRC, notification of the security breach was required to any individual affected by the breach.[50] In addition to notifying individuals affected, some US states require that the organisation notify the relevant

---

43 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 14. For example, California does not define encryption in the Civil Code. It has, however, issued guidelines recommending that data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.

44 Ibid, 14.

45 *Indiana Code* § 24-4.9-2-11. See also *Ohio Revised Code* § 1347.12(A)(9).

46 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

47 See, eg, *California Civil Code* § 1798.29(a); *Ohio Revised Code* § 1347.12(B)(1); *Delaware Code* § 12B-102(a); *Indiana Code* § 24-4.9-3-1; *New York State Code* § 899-44(2); *Arkansas Code* § 4-110-105. See also United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

48 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 25.

49 Ibid, 26.

50 See, eg, *California Civil Code* § 1798.29(a); *Ohio Revised Code* § 1347.12(B)(1); *Delaware Code* § 12B-102(a); *Indiana Code* § 24-4.9-3-1; *New York State Code* § 899-44(2); *Arkansas Code* § 4-110-105. See also United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

consumer protection agency.[51] The US Interagency Guidance provides that an institution should notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorised access to or use of 'sensitive personal information'.[52] Similarly, the CIPPIC recommended in its proposed model for Canada, that

> there should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, with full information about the nature and extent, the anticipated risks, mitigation measures, steps taken to notify affected individuals or, where notification is not considered warranted, the justification for not taking this step.[53]

47.35 Under the CIPPIC model, notice should be made to the Privacy Commissioner regardless of whether the test of individual notification is met. This would ensure that a record is kept of all security breaches, which provides oversight of organisational practices. It also 'offers the potential for organisations to obtain guidance from the Privacy Commissioner regarding notification obligations and methods'.[54] The CIPPIC also proposed that government agencies, credit bureaux and law enforcement authorities should be notified. The CIPPIC envisages that the Privacy Commissioner provide guidance to organisations as to which agencies should be notified in the context of a specific breach.[55]

Timing, method and content of notification

Timing of notification

47.36 In California, and most other US states with data breach notification laws, notification must occur in 'the most expedient manner possible and without unreasonable delay'.[56] The US Interagency Guidance provides that an institution must notify an affected customer 'as soon as possible' after concluding that misuse of the customer's information has occurred or is reasonably possible. Most US states, and the US Interagency Guidance, allow for delays in, or exceptions to, notification if notice will jeopardise a law enforcement investigation.

47.37 The CIPPIC proposal for Canada adopted similar timing for data breach notification. It proposed that notification should be undertaken 'as soon as possible and

---

51 See, eg, *Delaware Code* § 12B-102(d).

52 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

53 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 26.

54 Ibid, 26.

55 Ibid, 26–27.

56 *California Civil Code* § 1798.29(a).

without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay'.[57]

Method of notification

47.38 The general approach of US state data breach notification laws is to describe the method of notification. For example, the *California Civil Code* provides that notice may be provided by written notice and electronic notice.[58] Other US states also allow notice by telephone or facsimile.[59]

47.39 California also provides for substituted notice where the organisation demonstrates that the: cost of providing notice would exceed a $250,000; affected class of subject persons to be notified exceeds 500,000; or agency does not have sufficient contact information. Substituted notice consists of: email notice, where the organisation has an email address for the subject persons; conspicuous posting of the notice on the organisation's website page, if the organisation maintains a website; and notification to major statewide media.[60]

47.40 Most US states have developed similar substituted notice schemes to handle large security breaches.[61] While the threshold and methods for substituted notice vary between states, a number of US states have adopted the same requirements as California.[62] In contrast to these approaches, the US Interagency Guidance prescribes a more general requirement that notice should be delivered 'in any manner that is designed to ensure that a customer can reasonably be expected to receive it'.[63]

47.41 In the CIPPIC's proposed model, notification 'should generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met'.[64] In particular, email notice should only be allowed where the individual concerned has consented explicitly to receiving 'important notices such as this by email'. Substituted notice should be permitted where 'large numbers of individuals (eg, over 100,000) must be notified, where the total cost of individual notification is extraordinary (eg, over $150,000), or where the Privacy Commissioner has specifically

---

57 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 28.

58 *California Civil Code* § 1798.29(g).

59 See, eg, *New York State Code* § 899-aa(5)(c); *Indiana Code* § 24-4.9-3-4(a).

60 See, eg, *California Civil Code* § 1798.29(g)(3).

61 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 17.

62 See, eg, *Arkansas Code* § 4-110-105(2); *Ohio Revised Code* § 1347.12(E).

63 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005), 46.

64 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 28.

approved the substitute notice'.[65] The CIPPIC proposed similar substituted mechanisms as provided in the California data breach notification law.

Form and content of notification

47.42 California does not specify the contents of the actual data breach notice. In contrast, other US states and the US Interagency Guidance provide detail on what should be covered in a notice. The general approach is to require the following information:

- a general description of what occurred, including the time and date of the breach and when it was discovered;
- the type of personal information that was the subject of the unauthorised access, use or disclosure;
- contact information for affected individuals to obtain more information and assistance; and
- a reminder of the need to remain vigilant and to report promptly incidents of suspected identity theft to the organisation.[66]

47.43 In its proposal for a Canadian data breach notification law, the CIPPIC proposed that breach notices include similar matters as set out above. It also suggested that the notice

> should be separate from other communications and should include detailed information about the breach, including an assessment of the risk that the personal information of affected individuals will be used in an unauthorized manner.[67]

Penalties for failure to notify

47.44 Some US states provide penalties for failure to make a disclosure or notification in accordance with the applicable law. For example, the Indiana Code provides that any person that fails to comply with its data breach notification law 'commits a deceptive act that is actionable only by the Attorney General'.[68] The Attorney General

---

65 Ibid, 28.

66 See, eg, *New York State Code* § 899-aa(5)(c). Similar matters are included in United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005); Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

67 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007), 27.

68 *Indiana Code* § 24-4.9-4-1.

may bring an action to obtain an injunction or a civil penalty of not more than $150,000 per deceptive act.[69]

Submissions and consultations

General support

47.45 Many stakeholders, including the Office of the Privacy Commissioner (OPC), expressed general support for a requirement that data users notify individuals of a breach to their personal information in certain circumstances.[70] Supporters of a data breach notification law gave a number of reasons why such a law would be valuable. These include that it would:

- provide a strong market incentive and stimulus to organisations to secure databases adequately to avoid the brand and reputational damage arising from negative publicity;[71]
- encourage attention to compliance and vigilance against identity theft;[72] and
- improve accountability, openness and transparency in the handling of personal information by agencies and organisations.[73]

Opposing a data breach notification requirement

47.46 Some stakeholders stated expressly that there is no need for a data breach notification principle or requirement. Others submitted that the current principles were appropriate—implying that a data breach principle is not appropriate or necessary.[74]

---

69 Ibid § 24-4.9-4-2. See also *Arkansas Code* § 4-110-108.

70 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAMI, *Submission PR 147,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; Civil Liberties Australia, *Submission PR 98,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

71 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007.

72 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

73 Office of the NSW Privacy Commissioner, *Submission PR 193,* 15 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

74 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007; AXA, *Submission PR 119,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

47.47 The Australian Federal Police (AFP) submitted there should be no requirement to notify individuals about the misuse, loss or unauthorised access to, modification or disclosure of personal information. While recognising the benefit to the individual of notification, the AFP expressed concern that requiring notification may contribute to the already excessive caution exercised by agencies, organisations and individuals in relation to privacy.[75]

Triggers for reporting

47.48 A number of stakeholders identified the criteria for triggering the requirement to notify individuals affected by a data breach as a critical issue.[76] For example, the National Health and Medical Research Council submitted that the requirement to report should be qualified on the basis of the significance of the breach and the practicality and reasonableness of notifying individuals.[77] The idea of making the reporting proportionate to the potential for harm was supported by a number of stakeholders, including the OPC.

47.49 Microsoft Australia submitted, for example, that the trigger for requiring notification of a security breach should be if the 'breach could reasonably result in the misuse of that individual's unencrypted sensitive financial information'. Microsoft Australia argued that this test strikes

> an appropriate balance between empowering individuals to minimise the more serious consequences that might flow from a security breach involving their personal information, and avoiding a situation whereby security notifications are so frequent that individuals disregard them or are unable to differentiate between those that indicate a significant risk and those that don't.[78]

47.50 In terms of the type of notification, Microsoft Australia suggested that organisations should be afforded some discretion as to the method by which they provide breach notification to individuals. In particular, organisations should be able to take into account factors such as the size of their organisation; number of potential recipients of a notification; the relative cost of different methods of providing

---

75 Australian Federal Police, *Submission PR 186,* 9 February 2007.

76 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Microsoft Australia, *Submission PR 113,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

77 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007. See also Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

78 Microsoft Australia, *Submission PR 113,* 15 January 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

notification; and the ways in which the organisation typically communicates with its customers.[79]

47.51 The Office of the Victorian Privacy Commissioner stated that the starting point for breach notification in Victoria is the objects clause of the *Information Privacy Act 2000* (Vic), which provides that the collection and handling of personal information is to be 'responsible' and 'transparent'. Part of this obligation is to tell individuals 'when something goes wrong and to explain to them what has been done to try to avoid or remedy any actual or potential harm'.[80] There is a presumption, therefore, that privacy breaches ought to be notified to those whom they potentially affect. Only in exceptional cases should a senior decision-maker in possession of all the facts make the decision that notification is 'neither necessary nor desirable'. In deciding whether the circumstances of a case are exceptional, the decision maker should have regard to the following factors:

- the potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved;
- the potential for notification itself to cause reasonably foreseeable harm to the data subjects, excluding harm to those responsible for the breach; and
- whether, considering the two points above, notification is reasonably likely to alleviate more harm than it would cause.[81]

47.52 While not expressing direct support for a data breach notification requirement, Veda Advantage acknowledged that there may be a case for organisations that operate large, highly transactional databases to notify consumers and regulators in the event of a significant data loss or theft.[82]

47.53 The Law Council of Australia did not express support for a data breach notification requirement. The Law Council noted, however, that many organisations already report data breaches where they believe the information is confidential and disclosure could result in harm. In contrast, where a breach is internal and is quickly remedied so no harm could result, organisations would not necessarily disclose the breach, as disclosure may give rise to unjustified alarm on the part of the individual.[83]

---

79 Microsoft Australia, *Submission PR 113,* 15 January 2007.

80 Office of the Victorian Privacy Commissioner, *Guidelines to Victoria's Information Privacy Principles* (2nd ed, 2006), [4:77] as affirmed in Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007. Also referred to in Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.

81 Office of the Victorian Privacy Commissioner, *Guidelines to Victoria's Information Privacy Principles* (2nd ed, 2006), [4:77]–[4:78] as affirmed in Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

82 Veda Advantage, *Submission PR 163,* 31 January 2007.

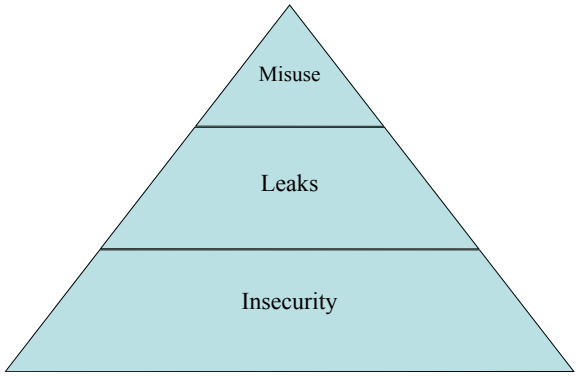
83 Law Council of Australia, *Submission PR 177,* 8 February 2007.

ALRC's view

47.54 In considering whether a data breach notification law is appropriate for Australia, the ALRC has had regard to the theoretical framework proposed by Professor Daniel Solove in dealing with information abuses, such as identity theft and fraud.[84] The ALRC has also considered the general objectives of regulation, as discussed by Professors Robert Baldwin and Martin Cave.[85]

Data abuse pyramid

47.55 Data breach notification should be considered within the context of the *Privacy Act*'s objective to protect the personal information of individuals. Solove has suggested that data security 'is quickly becoming one of the major concerns of the Information Age'.[86] Solove has developed a 'data abuse pyramid' in which 'to think about information abuses, their causes and the way they should be remedied'.[87] The pyramid represents how and why many types of information abuses occur, and is represented below.



47.56 At the top of the pyramid are actual 'misuses' of data—that is, when information is employed to carry out identity theft, fraud, or other activities. A level below misuse are 'leaks'—when entities improperly release or provide access to personal information. At the bottom of the pyramid is 'insecurity', which involves a general lack of protection accorded to personal data by entities.[88] Solove suggests that

84 D Solove, *The New Vulnerability: Data Security and Personal Information* (2005) George Washington University Law School Public Law Research Paper No 102.
85 See R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999).
86 D Solove, *The New Vulnerability: Data Security and Personal Information* (2005) George Washington University Law School Public Law Research Paper No 102, 1.
87 Ibid, 2.
88 Ibid, 2–3.

the law must become involved at the lower levels of the pyramid, rather than just responding to the top of the pyramid, by way of criminal sanctions for identity crimes.[89]

Data leaks

47.57 As Solove explains, 'with a leak, the harm consists in being exposed to the potential for being subjected to identity theft, fraud, or even physical danger'.[90] The *Privacy Act* does not provide any direct response to the second level of Solove's pyramid, where information has been 'leaked', or where there has been an unauthorised acquisition of personal information from an agency or organisation. As the Act currently stands, therefore, there is no obligation to inform individuals that their personal information has been accessed by an unauthorised person and that they may be at an increased risk of identity theft or fraud.

47.58 In the ALRC's view, the Act should provide notification to individuals affected by a security breach. The ALRC agrees with the central rationale given for data breach notification laws that notifying people that their personal information has been breached can help to minimise the damage caused by the breach.[91] Notification acknowledges the fact that a data breach can expose an individual to a potentially serious risk of harm and, by arming the individual with the necessary information, gives the individual the opportunity, for example, 'to monitor their accounts, take preventative measures such as new accounts, and be ready to correct any damage done'.[92] Early notification would also facilitate the ALRC's proposal in Chapter 52, that individuals be able to apply to credit reporting agencies to put a notice on their credit report that the individual has been the subject of identity theft.[93]

47.59 A legal requirement to notify, in contrast to a voluntary approach, is necessary because, as explained above, there is a risk that the uncontrolled market may 'undersupply notification'.[94] That is, because of the reputational damage that notification can cause, organisations may not have incentives to notify customers of a data breach voluntarily.[95]

---

89 Ch 9 discusses some of the offences and penalties for identity crime in Australia.

90 D Solove, *The New Vulnerability: Data Security and Personal Information* (2005) George Washington University Law School Public Law Research Paper No 102, 7.

91 See M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute; Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper* (2007).

92 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 3.

93 See Proposal 52–1.

94 M Turner, *Towards a Rational Personal Data Breach Notification Regime* (2006) Information Policy Institute, 13.

95 Ibid, 11.

Data insecurity

47.60 The *Privacy Act* contains provisions to address the problems identified at the base of Solove's pyramid, by requiring agencies and organisations to take reasonable steps to keep personal information secure. This is in contrast to many states in the US, which, as noted above, do not have broader legislation in place regulating the personal information handling practices of agencies or organisations.

47.61 In the ALRC's view, a data breach notification requirement can enhance the existing protections offered by the *Privacy Act* by providing incentives to improve data security, in compliance with the proposed 'Data Security' principle. The reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful deterrents against lax security.

47.62 Even more broadly, notification of security breaches can play an important role in keeping the market informed of the privacy practices of organisations. As Baldwin and Cave suggest, 'competitive markets can only function properly if consumers are sufficiently well informed to evaluate competing products'.[96] In the absence of notification, a data breach causes an 'information inadequacy', as the organisation knows that there has been an unauthorised acquisition of an individual's personal information, but the individual affected does not. Thus, until the individual is notified of a security breach, there may be inadequate information in the market for individuals to evaluate the different personal information-handling practices of organisations. Notification can provide insight into an organisation's security practices and help inform the market about the vulnerabilities or weaknesses of a particular organisation compared to others.

Trigger for notification

47.63 In the ALRC's view, the proposed data breach notification provisions should include a general requirement to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person; and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

47.64 There are several factors to note about this proposed triggering event. First, it sets a higher threshold for notification than is provided in the Californian test. Rather than requiring notification of 'any unauthorised acquisition' of personal information, the proposed test allows the agency or organisation to investigate the data breach and make an assessment of whether the unauthorised acquisition may give rise to a real potential for serious harm to an individual. Serious harm is not limited to identity theft

96 R Baldwin and M Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999), 12.

or fraud. The harm could include, for example, discrimination, if sensitive medical information was released.

47.65 Setting the threshold higher than an unauthorised acquisition should reduce the risk of 'notification fatigue', where individuals receive so many notices of data breaches that it becomes difficult for them to assess which ones carry a serious risk of harm and which ones are minor in nature and consequence. A higher threshold for notification should also reduce the compliance burden on agencies and organisations.

47.66 Secondly, while the agency or organisation is given primary responsibility for deciding whether the triggering event has occurred, the ALRC's proposal provides for oversight by the Privacy Commissioner. It is preferable that the decision about notification is made in consultation with the Privacy Commissioner, and that the Commissioner is able to require notification where he or she believes that the unauthorised acquisition gives rise to a real risk of serious harm to any affected individual, even if the agency or organisation disagrees. This oversight is similar to the model put forward by the CIPPIC and the Canadian Government Standing Committee on Access to Information, Privacy and Ethics. The Commissioner could also use this oversight power to require that notification be made to other bodies as appropriate, such as the major credit reporting agencies.[97]

47.67 Thirdly, consistently with the ALRC's proposal that the *Privacy Act* be technologically neutral,[98] the requirement to notify should not be restricted to computerised information, but should apply to any unauthorised access to personal information—whether through a lost laptop; a hacker accessing an organisation's electronic files; misplaced hard copy files; or careless disposal of hard copy personal information. This broad application should encourage compliance with the proposed 'Data Security' principle, which requires that agencies and organisations take reasonable steps to protect the information it holds and to destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the proposed Unified Privacy Principles (UPPs).

Exceptions

47.68 While the proposed triggering event set out above is narrower than that adopted in many states in the US, the ALRC acknowledges the concern expressed by stakeholders that there be some exceptions and discretion around the requirement to notify.

47.69 The ALRC proposes that the provisions should include an exception where the specified personal information was encrypted adequately. The requirement that encryption be 'adequate' implicitly requires that the encryption key was not also acquired by the unauthorised person—encryption will obviously not be adequate where

97 This would also facilitate Proposal 52–1.
98 See Proposal 7–1.

there is an easy means of decoding the information. This phrasing also avoids any need to specify exactly what type of encryption is adequate, which would be contrary to the ALRC's goal of making the *Privacy Act* technologically neutral. An assessment of adequacy will depend on the circumstances of the case, taking into account matters such as the type of personal information, the nature of the organisation holding it, and the risk of harm that would be caused by its unauthorised acquisition. The Privacy Commissioner should issue guidance on the type and standard of encryption he or she will generally consider adequate, and the factors he or she will consider in assessing whether an agency or organisation will be able to avail itself of this exception in the case of a data breach.

47.70 The ALRC proposes that the data breach notification provisions provide an exception to the requirement to notify where the information was acquired in good faith by an employee or agent where the agency or organisation was otherwise acting for a purpose permitted by the proposed UPPs—provided that the personal information is not used or subject to further unauthorised disclosure. This exception would apply to situations where, for example, an employee accidentally accesses specified personal information of a customer in the process of collecting information for a permitted purpose. It would not cover situations where an employee is acting outside a purpose permitted by the proposed UPPs, such as where he or she is 'snooping' or accessing personal information for illegitimate purposes.[99]

47.71 The ALRC also proposes that the Privacy Commissioner have a broad discretion to waive the notification requirement where the Commissioner does not consider that it would be in the public interest. This would cover situations where there is a law enforcement investigation being undertaken into the breach and notification would impede that investigation.

'Specified personal information' for the purposes of notification

47.72 As noted above, in US state data breach notification laws, only the combination of particular types of personal information gives rise to the obligation to notify. The US laws do not apply to the range of personal information which falls within the definition of 'personal information' in the *Privacy Act*.

47.73 In the ALRC's view, the *Privacy Act* should adopt a definition of 'specified personal information' for the purposes of the proposed data breach notification provisions. This definition should draw on the existing definitions of 'personal information' and 'sensitive information' in the *Privacy Act* and should prescribe what combinations of these types of information would, when acquired without authorisation, give rise to a real risk of serious harm so as to require notification.

---

99 See, eg, the 'Centrelink Staff Sacked over Breaches', *Sydney Morning Herald* (online), 22 August 2006, <www.smh.com.au>.

47.74 For example, adopting the approach of the US Interagency Guidance and CIPPIC definitions, 'specified personal information' could include information in electronic or paper form, which includes an individual's name or address, in combination with any of the following:

- driver's licence or proof of age;
- Medicare number—or new access card number if the legislation is passed;
- account numbers, credit or debit card numbers, or other unique identifiers issued by other organisations together with any security code, password or access code that would permit access to the individual's information; or
- sensitive information (as defined in the *Privacy Act*).

47.75 The unauthorised acquisition of any of these combinations of information could arm a person with sufficient personal information to commit both an 'account takeover' and 'true name fraud', as defined above. The ALRC recognises that this suggested definition of 'specified personal information' is not limited to financial information, as suggested by Microsoft Australia.[100] While preventing identity fraud is one of the key rationales for data breach notification, it is not the only consequence that can flow from an unauthorised acquisition of personal information. Discrimination, stalking, and other harmful consequences could potentially flow from a security breach. The proposed data breach notification provisions should therefore deal with a broader range of information than 'sensitive financial information'.

Other matters

47.76 At this stage, the ALRC has not specified in the proposal the form, content, method or timing of notification. As with the definition of 'specified personal information', however, there are elements of the US laws and CIPPIC proposal upon which the data breach notification law could be modelled, if the decision was made to implement such provisions in the *Privacy Act*.

Form of notification

47.77 In relation to the form of the breach notification, the ALRC agrees with the CIPPIC's proposal that data breach notification should be a stand-alone communication, and should not be attached to other correspondence from the agency or organisation. Including the notification with other correspondence, such as marketing material, may confuse individuals about the nature and seriousness of the notification, and may cause it to be 'lost in the bundle'.

---

100 See Microsoft Australia, *Submission PR 113,* 15 January 2007.

Content of notification

47.78 In the ALRC's view, the content of breach notification should address similar matters to those suggested in the US Interagency Guidance and CIPPIC proposal for Canada. In particular, the notification should provide:

- a description of the breach;
- a list of the type of personal information that was disclosed;
- an assessment of the risk of identity fraud as a result of the breach and steps the individual can take to help mitigate that risk; and
- contact information for affected individuals to obtain more information and assistance.

Method of notification

47.79 Ordinarily, a breach notification should be directed personally to the individual affected. Rather than prescribing the various methods by which an agency or organisation can notify an individual, in the ALRC's view, it would be preferable to allow for the method of notification to be determined by the agency's or organisation's ordinary method of communicating with the individual. If, for example, an agency or organisation usually corresponds with an individual through by post, then it should not provide notification by email. Agencies and organisations should also be able to have regard to any arrangements they have in place for contacting an individual in an emergency situation.

47.80 In relation to substituted notice, the ALRC does not propose to set a particular threshold for allowing substituted notice, in terms of cost of notification or number of people to notify. It would be difficult to set a threshold that would be fair and reasonable to all the agencies and organisations subject to the *Privacy Act*, particularly if the small business exemption were removed. In the ALRC's view, it would be preferable to empower the Privacy Commissioner to approve substituted notice where he or she believes it is appropriate, reasonable and fair in all the circumstances.

Timing of notification

47.81 In the ALRC's view, notification should occur as soon as reasonably practicable after notification to the OPC. As noted above, under the proposed provisions the Commissioner would have discretion to delay or exempt notification for law enforcement purposes.

Penalties

47.82 In the ALRC's view, failure to comply with the proposed data breach notification provisions should attract a civil penalty. This would provide a strong incentive for agencies and organisations to disclose data breaches where required, and should act to encourage agencies and organisations to consult with the OPC where a data breach has occurred to ensure they are in full compliance with the requirements.[101] The presence of civil penalties should also provide incentives to train staff adequately to ensure that laptops are not left in airports, hard files are not left unsecured, electronic and hard copy information is appropriately disposed of, and electronic information is encrypted and secured adequately.

Proposal 47–1 The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:

(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

(b) An agency or organisation is not required to notify any affected individual where:

  (i) the specified information was encrypted adequately;

  (ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy Principles (provided that the personal information is not used or subject to further unauthorised disclosure); or

  (iii) the Privacy Commissioner does not consider that notification would be in the public interest.

(c) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

101 See B Arnold, 'Losing It: Corporate Reporting on Data Theft' (2007) 3 *Privacy Law Bulletin* 101, 103.

Australian Government
Australian Law Reform Commission

Review of Australian Privacy Law

DISCUSSION PAPER

You are invited to provide a submission or comment on this Discussion Paper

VOLUME 3
DISCUSSION PAPER 72
SEPTEMBER 2007

This Discussion Paper reflects the law as at 31 July 2007

ISBN- 978-0-9758213-9-8

Commission Reference: DP 72

The Australian Law Reform Commission was established on 1 January 1975 by the *Law Reform Commission Act 1973* (Cth) and reconstituted by the *Australian Law Reform Commission Act 1996* (Cth). The office of the ALRC is at Level 25, 135 King Street, Sydney, NSW, 2000, Australia.

All ALRC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the ALRC.

Telephone:	within Australia	(02)	8238 6333
	International	+61 2	8238 6333
TTY:		(02)	8238 6379
Facsimile:	within Australia	(02)	8238 6363
	International	+61 2	8238 6363

E-mail: info@alrc.gov.au

ALRC homepage: www.alrc.gov.au

Printed by Ligare Pty Ltd

Summary of Contents

Volume 1

Part A – Introduction 101

1. Introduction to the Inquiry 103
2. Overview—Privacy Regulation in Australia 145
3. The *Privacy Act* 169
4. Achieving National Consistency 235
5. Protection of a Right to Personal Privacy 277

Part B – Developing Technology 309

6. Overview—Impact of Developing Technology on Privacy 311
7. Accommodating Developing Technology in a Regulatory Framework 341
8. Individuals, the Internet and Generally Available Publications 375
9. Identity Theft 393

Part C – Interaction, Inconsistency and Fragmentation 404

10. Overview—Interaction, Inconsistency and Fragmentation 405
11. The Costs of Inconsistency and Fragmentation 419
12. Federal Information Laws 447
13. Required or Authorised by or under Law 487
14. Interaction with State and Territory Laws 519

Volume 2

Part D – The Privacy Principles 541

15. Structural Reform of Privacy Principles 543
16. Consent 571

17. Anonymity and Pseudonomity **587**
18. Collection **599**
19. Sensitive Information **613**
20. Specific Notification **627**
21. Openness **651**
22. Use and Disclosure **667**
23. Direct Marketing **699**
24. Data Quality **719**
25. Data Security **729**
26. Access and Correction **755**
27. Identifiers **775**
28 Transborder Data Flows **815**
29. Additional Privacy Principles **865**

Part E – Exemptions 875

30. Overview—Exemptions from the *Privacy Act* **877**
31. Defence and Intelligence Agencies **899**
32. Federal Courts and Tribunals **927**
33. Exempt Agencies under the *Freedom of Information Act 1982* (Cth) **955**
34. Other Public Sector Exemptions **975**
35. Small Business Exemption **1007**
36. Employee Records Exemption **1039**
37. Political Exemption **1065**
38. Media Exemption **1081**
39. Other Private Sector Exemptions **1113**
40. New Exemptions **1123**

Part F – Office of the Privacy Commissioner 1141

41. Overview—Office of the Privacy Commissioner **1143**
42. Facilitating compliance with the *Privacy Act* **1151**
43. Structure of the Office of the Privacy Commissioner **1159**

44. Powers of the Office of the Privacy Commissioner 1185
45. Investigation and Resolution of Privacy Complaints 1239
46. Enforcing the *Privacy Act* 1275
47. Data Breach Notification 1293

Volume 3

Part G – Credit Reporting Provisions 1321
48. Overview—Credit Reporting 1323
49. The Credit Reporting Provisions 1337
50. The Approach to Reform 1359
51. More Comprehensive Credit Reporting 1401
52. Collection of Credit Reporting Information 1445
53. Use and Disclosure of Credit Reporting Information 1475
54. Data Quality and Security 1503
55. Rights of Access, Complaint Handling and Penalties 1529

Part H – Health Services and Research 1557
56. Regulatory Framework for Health Information 1559
57. The Privacy Act and Health Information 1595
58. Research 1653

Part I – Children, Young People and Adults Requiring Assistance 1713
59. Children, Young People and Privacy 1715
60. Decision Making by Individuals Under the Age of 18 1751
61. Adults with a Temporary or Permanent Incapacity 1815
62. Other Third Party Assistance 1839

Part J – Telecommunications **1847**

63. *Telecommunications Act* **1849**

64. Other Telecommunications Privacy Issues **1901**

Part G

Credit Reporting Provisions

48. Overview—Credit Reporting

Contents

Introduction 1323
What is credit reporting? 1325
Credit reporting agencies 1327
Background to national regulation 1328
State legislation 1328
New regulatory momentum 1330
Legislative history 1331
Privacy Amendment Bill 1989 1331
Senate deliberations 1332
Privacy Amendment Act 1990 1333
Credit Reporting Code of Conduct 1334
Subsequent amendments 1334

Introduction

48.1 The *Privacy Amendment Act 1990* (Cth), which commenced operation in September 1991, extended the coverage of the *Privacy Act* to consumer credit reporting. The credit reporting provisions of the *Privacy Act 1988* (Cth) are contained in Part IIIA and associated provisions (the credit reporting provisions).[1]

48.2 The credit reporting provisions regulate the collection, use and disclosure of personal information concerning credit that is intended to be used wholly or primarily for domestic, family or household purposes.[2] Commercial credit information is only incidentally regulated by the Act, for example, where it is used to assess an application for consumer credit.[3]

48.3 Part G examines the credit reporting provisions and makes proposals for reform. This chapter introduces the topic by describing the role of credit reporting, the background to the national regulation of credit reporting through the *Privacy Act*, and the legislative history of the credit reporting provisions.

---

1 The major associated provisions include definitions and interpretation provisions: *Privacy Act 1988* (Cth) ss 6, 11A and 11B; and provisions dealing with the *Credit Reporting Code of Conduct*: ss 18A; 18B.

2 See the definitions of 'commercial credit' and 'credit': Ibid s 6(1).

3 Ibid s 18L(4).

48.4 Chapter 49 provides a summary of the content of the credit reporting provisions, the responsibilities and powers of the Office of the Privacy Commissioner (OPC) with regard to credit reporting,[4] and the remedies and penalties available in the event of non-compliance with the credit reporting provisions.[5]

48.5 Chapter 50 introduces the ALRC's proposals for reform of the credit reporting provisions. The chapter summarises views expressed in submissions and consultations about the operation of existing regulation. The ALRC proposes that the credit reporting provisions of the *Privacy Act* be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and proposed Unified Privacy Principles (UPPs).[6]

48.6 The ALRC proposes, in Chapter 50, that privacy rules, which impose obligations on credit reporting agencies and credit providers in respect to the handling of credit reporting information, be promulgated in regulations under the *Privacy Act*—the *Privacy (Credit Reporting Information) Regulations*. The ALRC also makes a range of other proposals concerning the general approach to the drafting and application of the *Privacy (Credit Reporting Information) Regulations* and proposes that the regulations be supplemented by a credit reporting industry code.

48.7 Chapter 51 considers proposals to extend the current system of credit reporting to permit a broader spectrum of personal information to be collected and disclosed—referred to in this Discussion Paper as 'more comprehensive' credit reporting. The chapter examines the arguments for and against more comprehensive credit reporting, with particular reference to comments received in submissions and consultations, and information derived from empirical research into the possible effects of more comprehensive credit reporting on credit markets and the economy. The ALRC proposes a modest extension in the categories of personal information that may be collected for credit reporting purposes.

48.8 Chapter 52 discusses the collection of credit reporting information, the permissible content of credit reporting information and notification of collection. The ALRC makes a range of proposals in relation to, among other things, regulating the collection of information about identity theft, personal insolvency, serious credit infringements and debts of children and young people. The imposition of more prescriptive notice requirements is also proposed.

48.9 Chapter 53 discusses issues concerning the use and disclosure of credit reporting information. The ALRC makes a range of proposals concerning the relationship between the proposed 'Use and Disclosure' principle of the UPPs and the proposed *Privacy (Credit Reporting Information) Regulations*, and regulating the use and disclosure of credit reporting information in direct marketing and identity verification.

---

4 The powers and responsibilities of the OPC generally are discussed in Part F.
5 The remedies and penalties available under the Act generally are discussed in Part F.
6 As discussed in Part D.

The chapter also considers the role of individual consent to the use and disclosure of credit reporting information.

48.10 Chapter 54 discusses the data quality and security of credit reporting information. The ALRC makes a range of proposals in relation to regulating the reporting of statute-barred debts, overdue payments, and schemes of arrangement, and to improve data quality generally. The chapter also discusses the deletion of credit reporting information after maximum permissible periods of retention and data security.

48.11 Chapter 55 discusses individual rights of access to, and correction of, credit reporting information. Proposals are made setting out how these matters should be dealt with under the proposed UPPs and the *Privacy (Credit Reporting Information) Regulations*. The ALRC examines complaint handling in credit reporting disputes by the OPC and other complaint-handling mechanisms, and penalties for breach of the regulations. Importantly, the ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where the credit provider is a member of an external dispute resolution scheme approved by the OPC.

What is credit reporting?

48.12 Credit reporting involves providing information about an individual's credit worthiness to banks, finance companies and other credit providers, such as retail businesses that issue credit cards or allow individuals to have goods or services on credit. Credit reporting is generally conducted by specialised credit reporting agencies that collect and disclose information about potential borrowers, usually in order to assist credit providers to assess applications for credit.

48.13 Credit reporting agencies collect information about individuals from credit providers and publicly available information (such as bankruptcy information obtained from the Insolvency and Trustee Service Australia—a federal government agency). This information is stored in central databases for use in generating credit reporting information for credit providers. In assessing credit applications, this information augments information obtained directly from an individual's application form and the credit provider's own records of past transactions involving the individual.

48.14 The information contained in credit reporting databases may be used in credit scoring systems. Credit scoring may be described as the use of 'mathematical algorithms or statistical programmes that determine the probable repayments of debts

by consumers, thus assigning a score to an individual based on the information processed from a number of data sources'.[7]

48.15 More generally, credit reporting agencies provide information processing services that assist credit providers to assess credit applications. One agency, Veda Advantage stated that:

> Statistical modelling of individual's behaviour over significant timeframes has enabled Veda Advantage to provide its customer base with the credit file characteristics which are statistically relevant to the probability of default. Customisation of these credit file and behavioural characteristics by each subscriber is based on the particular risk model, portfolio and competitive positioning.[8]

48.16 As Professor Daniel Solove explains, credit reporting is an understandable response to a modern, interconnected world containing 'billions of people' and where 'word-of-mouth is insufficient to assess reputation'. He goes on to state:

> Credit reporting allows creditors to assess people's financial reputations in a world where first-hand experience of the financial condition and trustworthiness of individuals is often lacking.[9]

48.17 The role of a credit reporting agency is to provide rapid access to accurate and reliable standardised information on potential borrowers. Such information enables credit providers to manage the risks of lending and to guard against identity fraud. In economic theory, it is said that:

> Credit reporting addresses a fundamental problem of credit markets: asymmetrical information between borrowers and lenders that leads to adverse selection and moral hazard.[10]

48.18 Information asymmetry refers to the fact that, because a credit provider often cannot know the full extent of an applicant individual's credit history, the individual has more information about his or her credit risk than the credit provider. Adverse selection arises where a credit provider, operating in response to information asymmetry, prices credit based on the *average* credit risk of individuals. This creates an incentive for high risk applicants to apply (the price is low to them) and low risk applicants to reject credit (it is overpriced for them).

> The result is adverse selection because the client group the credit provider ends up with is a higher risk than the credit provider priced for. Better information allows credit providers to more accurately measure borrower risk and set loan terms accordingly, which is why credit providers maintain their own databases of

---

7 F Ferretti, 'Re-thinking the Regulatory Environment of Credit Reporting: Could Legislation Stem Privacy and Discrimination Concerns' (2006) 14 *Journal of Financial Regulation and Compliance* 254, 261.

8 Veda Advantage, *Submission PR 272,* 29 March 2007.

9 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 507–508.

10 M Miller, 'Introduction' in M Miller (ed) *Credit Reporting Systems and the International Economy* (2003) 1, 1.

information on a consumer but also seek out information shared by other credit providers and supplied to them by a credit reporting agency.[11]

48.19 Information asymmetry also creates moral hazard. A credit applicant may obtain credit fraudulently by failing to disclose his or her credit history. Credit reporting reduces moral hazard because non-payment to one credit provider can inform the actions of other credit providers.[12]

48.20 While the major purpose of credit reporting is to provide information to assist credit providers to assess applications for credit, credit reporting also may be seen as serving the associated purpose of facilitating responsible lending. That is, the information provided by credit reporting to credit providers may help to prevent individuals becoming financially overcommitted. Credit reporting also assists in trade and mortgage insurance and in debt collection.

Credit reporting agencies

48.21 At present, there are three main credit reporting agencies operating in the Australian market. These are—in order of market share—Veda Advantage, Dun and Bradstreet and Tasmanian Collection Service.

48.22 The major consumer credit reporting agency is Veda Advantage (previously named Baycorp Advantage), which states that it maintains credit worthiness related data on more than 13 million individuals in Australia and New Zealand.[13] It has over 5,000 subscribers from a wide range of industries, including banking, finance telecommunications, retail, utilities, trade credit, government, credit unions and mortgage lenders.[14]

48.23 Veda Advantage's Australian credit reporting business commenced in 1968 as the Credit Reference Association of Australia (CRAA), which was established by the finance industry.[15] As discussed below, the CRAA played a central role in developments leading to the enactment of the credit reporting provisions of the *Privacy Act*.[16]

---

11 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 247.

12 M Miller, 'Introduction' in M Miller (ed) *Credit Reporting Systems and the International Economy* (2003) 1, 1.

13 Veda Advantage, *About Veda—Value to Society* (2007) <www.mycreditfile.com.au> at 1 August 2007.

14 Veda Advantage, *Submission PR 163,* 31 January 2007.

15 Veda Advantage, *Frequently Asked Questions—Who is Veda Advantage?* (2007) Baycorp Advantage <www.mycreditfile.com.au> at 1 August 2007.

16 The following background to the enactment of the *Privacy Act* credit reporting provisions is drawn primarily from an article prepared by Roger Clarke, then chair of the Economic, Legal and Social Implications Committee of the Australian Computer Society: R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society; and from annual reports of the New South Wales Privacy Committee: New South Wales Government Privacy Committee, *Annual Report 1984* (1984); New South Wales Government Privacy Committee, *Annual Report* (1989).

Background to national regulation

48.24 There is a near universal view that the practice of credit reporting should be regulated. There are many reasons for this. One is that it vindicates an individual's right to privacy—as Professor Solove puts it, '[p]eople expect certain limits on what is known about them and on what others will find out'.[17] Another justification is that a credit report, which contains aggregated personal data, can be used to make decisions that 'profoundly affect a person's life'.[18] As such, there is special urgency in ensuring that it is accurate and not misused.

State legislation

48.25 The first Australian legislation regulating aspects of credit reporting was enacted in 1971. In Queensland, Part III Division I of the *Invasion of Privacy Act 1971* (Qld) established a licensing scheme for credit reporting agents. The Act included statutory provisions dealing with the:

- permissible purposes of credit reports;
- information to be furnished to consumers and credit reporting agencies when credit is refused on the basis of a credit report;
- information to be disclosed by credit reporting agencies on request by consumers; and
- obligations on credit reporting agencies to investigate and correct inaccurate information and delete old information.[19]

48.26 The *Invasion of Privacy Act* contained offences in relation to: obtaining information falsely from a credit reporting agency; unauthorised disclosure of credit reporting information; supplying false credit reporting information; and demanding payment by making threats in relation to credit-related information.[20] The credit reporting provisions of the Act were repealed in 2002.[21]

48.27 South Australia enacted the *Fair Credit Reports Act 1975* (SA), which provided individuals with rights of access and correction; required credit reporting agencies to adopt procedures to ensure the accuracy and fairness of consumer reports; and required

17 D Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 508.
18 Ibid, 508.
19 *Invasion of Privacy Act 1971* (Qld) ss 16, 17, 18, 24.
20 Ibid ss 19, 20, 21, 22, 25.
21 *Tourism, Racing and Fair Trading (Miscellaneous Provisions) Act 2002* (Qld) s 45.

traders to inform individuals of their use of adverse information in such reports.[22] The Act was repealed in 1987.[23]

48.28 In Victoria, the *Credit Reporting Act 1978* (Vic) provides consumers with rights of access to copies of files held in relation to them by a credit reporting agency and provides a mechanism to dispute details and request the amendment of incorrect information. Credit reporting regulations were made in 1978 to prescribe procedures and time limitations to be followed by consumers seeking to amend personal credit reports held by credit agents.[24] The Victorian Consumer Credit Review recently noted that:

> With the commencement of the [federal] *Privacy Act*, however, it appears that the continuing relevance of the Victorian Act declined because the *Privacy Act* was binding on the industry and more comprehensive for consumers.[25]

48.29 Australia's first privacy regulator, the New South Wales Privacy Committee, identified credit reporting as an important privacy issue.[26] In 1976, concerns about the privacy of credit reporting information led the Privacy Committee and the CRAA to enter a so-called 'Voluntary Agreement' under which the CRAA would provide individuals with access to the information it held about them.[27]

48.30 Despite the Voluntary Agreement, few incentives existed to encourage CRAA's credit provider subscribers to comply with the Voluntary Agreement, notify individuals about adverse reports and rights of access, or to ensure that information they provided to the CRAA was accurate and complete.[28] Some observers expressed serious doubts about the willingness and ability of the CRAA to discipline its member credit providers.

> Few clients appear to have ever been suspended, had their memberships cancelled, or had specific employees suspended, for breach of CRAA rules. In 1985, when the Secretary of a Hibernian Credit Union was found to have made an enquiry for purposes other than credit granting (and in the process invented an application for a $50,000 mortgage loan), CRAA failed to discipline either its client or the client's employee (NSW Privacy Committee Annual Report, 1985, 92–98). Even a Report to Parliament, the NSW Privacy Committee's ultimate sanction, had no effect.[29]

---

22 *Fair Credit Reports Act 1975* (SA) pt II.
23 *Statutes Amendment (Fair Trading) Act 1987* (SA) s 16.
24 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 266.
25 Ibid, 266.
26 Established under the *Privacy Committee Act 1975* (NSW).
27 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 4.
28 Ibid, 4–5.
29 Ibid, 5.

48.31 During 1983, the New South Wales Privacy Committee reviewed its experience with the Voluntary Agreement and concluded that self-regulation of the credit reporting industry was ineffective. The Committee made proposals that it hoped would be the basis of fair credit reporting legislation or a code of practice under consumer protection legislation.[30] The Committee stated that this position was in line with its view that the 'time is now ripe for information privacy legislation'.[31]

48.32 In 1989, Roger Clarke stated:

> Judging by the last decade's complaints and enquiries to the country's only long-standing privacy 'watchdog', the NSW Privacy Committee, the public regards consumer credit reporting as the largest single information privacy issue.[32]

New regulatory momentum

48.33 The momentum for regulation of credit reporting intensified in the late 1980s. In large part this was in response to proposals by the CRAA to implement a new system of credit reporting. This system was referred to by the CRAA as the Payment Performance System (PPS) and was described by the CRAA and others as a form of 'positive' reporting.[33]

48.34 In the 1980s, credit reporting in Australia did not involve the collection or disclosure in credit reports of so-called 'positive' information about an individual's credit position. Apart from publicly available information about bankruptcies and court judgments, credit information was restricted to default reports made by CRAA members—that is, 'negative' information.

48.35 During the latter part of 1988, CRAA publicised an intention to augment its collection of credit reporting information by including information about individuals' current credit commitments. The nature of the proposal was summarised by Clarke as follows:

> Under PPS, credit providers would supply CRAA with tapes containing their customers' credit accounts. This data would be merged with previously recorded data every 30 to 60 days. Reports would then contain a complete listing of all known credit accounts, balances owing (at some recent point in time), and the consumer's payment performance on every account during the previous 24 payment periods … Payments 120 days or more overdue would result in a default report being generated automatically.[34]

---

30 New South Wales Government Privacy Committee, *Annual Report 1984* (1984), 30.

31 Ibid, 31.

32 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 2.

33 As discussed in Ch 51, the ALRC is of the view that such systems are better described as 'comprehensive' or 'more comprehensive' credit reporting.

34 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 6.

48.36 The CRAA's proposals intensified concern about its operations. In 1989, the New South Wales Privacy Committee concluded that the CRAA proposals represented a 'new and significant threat to privacy' and again recommended regulation of credit reporting.[35] In April 1989, CRAA announced that it would postpone the introduction of the PPS until January 1990, at the request of the Commonwealth Minister for Consumer Affairs, the Hon Senator Nick Bolkus.

48.37 On 19 April 1989, a 'Summit' was sponsored by the Australian Privacy Foundation. The meeting was attended by federal parliamentarians, CRAA representatives, state government agencies, credit providers, consumer and civil liberties groups and the Australian Computer Society.[36] At the conclusion of the Summit, the Minister for Consumer Affairs announced that the Australian Government intended to extend the *Privacy Act* to cover consumer credit reporting. Credit reporting would therefore become subject to national legislation for the first time.

Legislative history

48.38 As enacted, the *Privacy Act* had limited application to the private sector. The Act set out the Information Privacy Principles (IPPs), which regulated the collection, handling and use of personal information by Commonwealth public sector agencies.[37] The Act also provided guidelines for the collection, handling and use of individual tax file number information in both the public and private sectors following enhancements in the use of this unique identifier in 1988.[38]

Privacy Amendment Bill 1989

48.39 The Privacy Amendment Bill 1989 was introduced on behalf of the Minister for Consumer Affairs on 16 June 1989. The second reading speech stated that:

> The Privacy Amendment Bill 1989 is the next step in the Government's program to introduce comprehensive privacy protection for the Australian community. The principal purpose of this Bill is to provide privacy protection for individuals in relation to their consumer credit records.[39]

48.40 To this end, the Bill adapted information privacy principles to provide privacy protection for individuals in relation to their personal information held by the consumer credit reporting industry.

---

35 New South Wales Government Privacy Committee, *Annual Report* (1989), 23.

36 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, 6.

37 Since 1994, the IPPs also cover ACT public sector agencies: *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).

38 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).

39 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

> At the present time, there are inadequate controls on consumer credit reporting agencies to prevent them from using their databases for non consumer credit purposes.[40]

48.41 The Bill was intended to regulate the collection, storage, access to, correction of, use and disclosure of personal credit information by credit providers and credit reporting agencies. These provisions would be supported by a code of conduct applying to information held in, or disseminated from, a central database and to the transfer of information between industry participants.[41] The Bill also provided individuals with an enforceable right of access to, and correction of, their credit records.

48.42 Significantly, the Bill restricted the categories of information that credit reporting agencies were permitted to include in individuals' credit information files. Essentially, credit reporting agencies were limited to collecting the kinds of information that they already held.[42]

48.43 The second reading speech highlighted public concern about the privacy implications of a more comprehensive form of credit reporting. It was said that 'the credit reporting agency would effectively become a central clearing house of information about the current financial commitments of all Australians'.

> Positive reporting would constitute a major change in the level of information collected on individuals. While the notion of information collected in a centralised agency is not new, the collection of personal information on individuals' spending habits is—credit and spending profiles of individuals would have been built up through all their credit transactions.[43]

48.44 The Australian Government did not consider that there was 'any proven substantial benefit from positive reporting proposals'. In view of such strong privacy concerns, it concluded that any such expansion was 'impossible to condone'.[44]

Senate deliberations

48.45 The Privacy Amendment Bill 1989 was the subject of intense debate in the Senate. During the passage of the Bill, some 120 amendments from the Government, the Opposition and the Australian Democrats were proposed.[45]

48.46 On 2 November 1989, the Minister for Consumer Affairs tabled amendments to the Bill as introduced. These amendments were the result of consultations with the

---

40 Ibid.
41 Ibid.
42 The permitted content of credit information files is discussed in Chs 51–52.
43 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).
44 Ibid.
45 Commonwealth, *Parliamentary Debates*, Senate, 12 November 1990, 3939 (M Tate—Minister for Justice and Consumer Affairs).

credit reporting industry and consumer and privacy groups and were said to clarify aspects of the regulatory scheme.[46]

48.47 Specifically, the amendments were intended to:

- widen the classes of businesses that would be able to access a credit reporting agency;
- enable credit information to be used to assist credit providers in combating serious credit infringements and in collecting debts; and
- allow commercial and consumer credit reports to be cross-referenced by credit providers when making lending decisions.[47]

48.48 Following the return of the Hawke Government in March 1990, the Privacy Amendment Bill 1989 was restored to the Senate Notice Paper on 31 May. On 23 August 1990, the Bill was referred to the Senate Standing Committee on Legal and Constitutional Affairs (the Senate Standing Committee) for inquiry and report.

48.49 The Senate Standing Committee report, recommending 64 amendments to the legislation, was presented to the Senate on 22 October 1990.[48] In debate on 12 November, the Government moved 23 modifications to the amendments recommended in the report.[49]

48.50 The Bill received a third reading, before passing with the support of the Democrats and the independent Senator Brian Harradine. The Bill was returned from the House of Representatives without amendment on 6 December 1990.

Privacy Amendment Act 1990

48.51 The *Privacy Amendment Act 1990* (Cth) received Royal Assent on 24 December 1990. The Privacy Amendment Bill 1989 had been described by the CRAA as containing 'the most restrictive credit reference laws in the Western world'.

> The credit industry launched a concerted campaign against the Bill, and obtained numerous amendments, but the 1989 Bill remained substantially intact when enacted.[50]

---

46 Commonwealth, *Parliamentary Debates*, Senate, 2 November 1989, 2788 (N Bolkus—Minister for Consumer Affairs).

47 Ibid. See also, Supplementary Explanatory Memorandum, Privacy Amendment Bill 1989 (Cth).

48 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *The Privacy Amendment Bill 1989 [1990]* (1990).

49 Commonwealth, *Parliamentary Debates*, Senate, 12 November 1990, 3927 (B Cooney).

50 G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672, 672.

48.52 Heralding the enactment of the legislation, Professor Graham Greenleaf noted that the credit reporting industry, in attempting to expand its activities into more comprehensive reporting, had 'provoked a degree of legislative control which it had avoided in the past'.[51] The legislation not only limited further expansion of credit reporting but was seen as 'rolling back the clock' by restricting certain existing practices, such as the provision of credit reports to real estate agents to check prospective tenants and mercantile agents to search for debtors' addresses.[52]

> It is rare for privacy legislation in any country to attempt such a retrospective repeal of the extension of data surveillance … This is the major achievement of the legislation: as a matter of public policy, it rejects the development of a multi-purpose reporting system as an unacceptable invasion of privacy—at least in the private sector.[53]

48.53 In order to allow the credit reporting industry time to comply with the new regulatory scheme, and to permit the Privacy Commissioner to issue a credit reporting code of conduct,[54] the Act did not commence operation until 24 September 1991. Before that date, transitional provisions were enacted,[55] deferring the commencement of the credit reporting provisions and the obligation to comply with the *Credit Reporting Code of Conduct* until 25 February 1992.[56]

Credit Reporting Code of Conduct

48.54 On 11 September 1991, the federal Privacy Commissioner issued the *Credit Reporting Code of Conduct* under s 18A of the *Privacy Act*. As required by the Act, the Privacy Commissioner consulted with government, commercial, consumer and other relevant bodies and organisations during the development of the Code. The Code became fully operational in February 1992 and was amended in 1995. Since then, amendments to the *Credit Reporting Code of Conduct* and explanatory notes have been made periodically, including to take into account changes made to the credit reporting provisions of the *Privacy Act*.[57]

Subsequent amendments

48.55 Amendments were made to the credit reporting provisions even before the *Privacy Amendment Act 1990* commenced operation. The *Law and Justice Legislation Amendment Act 1991* (Cth)[58] made amendments, among other things, to

---

51 Ibid, 672.
52 Ibid, 674.
53 Ibid, 674.
54 As required by *Privacy Act 1988* (Cth) s 18A(1).
55 *Law and Justice Legislation Amendment Act 1991* (Cth) s 21.
56 Unless an act or practice breached *Privacy Act 1988* (Cth) ss 18H–18J concerning individuals' access to credit information files and credit reports and the obligations of credit reporting agencies and credit providers to alter files and reports to ensure accuracy.
57 See, Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), 2.
58 *Law and Justice Legislation Amendment Act 1991* (Cth) pt 3, ss 10–20.

- clarify the definition of 'credit reporting business';
- provide that agents of credit providers can be treated as credit providers;
- permit individuals to authorise other persons to have access to their credit information file or credit report;
- ensure that credit providers can consider telephone applications for credit;
- permit information to be used for internal management purposes by credit providers;
- provide for notices in the case of joint applications for credit; and
- permit disclosure of personal information by credit providers to guarantors, mortgage insurers, dispute resolution bodies, in credit card and EFTPOS transactions and mortgage securitisation.

48.56 Since the commencement of the *Privacy Amendment Act 1990*, there have been a series of amendments to the credit reporting provisions. The first set of amendments was contained in the *Law and Justice Legislation Amendment Act (No 4) 1992* (Cth) and related to securitisation, then a relatively new development in the financial sector. Securitisation refers to a complex method of financing loans under which, for example, a mortgage financed ostensibly by a credit provider, such as a credit union or building society, ultimately may be financed under mortgage securitisation using funds invested by investors in a trust.[59] Although the credit reporting provisions of the *Privacy Act* already made some provision for securitisation, it was necessary to substitute these provisions with more comprehensive ones given the complexity of the industry.[60]

48.57 The *Law and Justice Legislation Amendment Act 1993* (Cth) amended provisions governing disclosure of credit information by credit providers to state and territory authorities that administer mortgage assistance schemes to facilitate the giving of mortgage credit to individuals.

48.58 The *Law and Justice Legislation Amendment Act 1997* (Cth) amended the credit reporting provisions to:

- insert a definition of the term 'guarantee';

---

59 Explanatory Memorandum, Law and Justice Legislation Amendment Bill (No 4) 1992 (Cth).
60 Ibid.

- give the Privacy Commissioner the power to determine that a federal agency is a credit provider; and

- allow an overdue payment under a guarantee to be listed on the guarantor's credit information file.

48.59 The *Financial Sector Reform (Amendments and Transitional Provisions) Act (No 1) 1999* (Cth) changed the definition of credit provider in s11B by repealing s11B(1)(b)(i) and (ii), which referred to building societies and credit unions respectively.

48.60 The *Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001* (Cth) amended various offence provisions under Part IIIA to require an intention to breach certain provisions of Part IIIA, as distinct from reckless or misleading behaviour.

48.61 Most recently, amendments providing for non-disclosure of reports made to certain law enforcement agencies under s 18K(5) were made by the *National Crime Authority Legislation Amendment Act 2001* (Cth), *Australian Crime Commission Establishment 2002* (Cth) and *Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006* (Cth).

49. The Credit Reporting Provisions

Contents

Introduction 1337
Application of the credit reporting provisions 1339
Information covered by the provisions 1339
Persons within the ambit of the provisions 1340
Content of credit information files 1342
Accuracy and security of personal information 1345
Disclosure of personal information 1346
Credit reporting agencies 1346
Credit providers 1348
Information given by credit providers to credit reporting agencies 1350
Use of personal information 1350
Credit providers 1350
Use and disclosure by mortgage and trade insurers 1351
Use and disclosure by other persons 1351
Rights of access, correction and notification 1352
Responsibilities and powers of the OPC 1353
Credit Reporting Code of Conduct 1353
Determinations 1355
Audits of credit information files 1356
Investigating credit reporting infringements 1356
Remedies and penalties 1358

Introduction

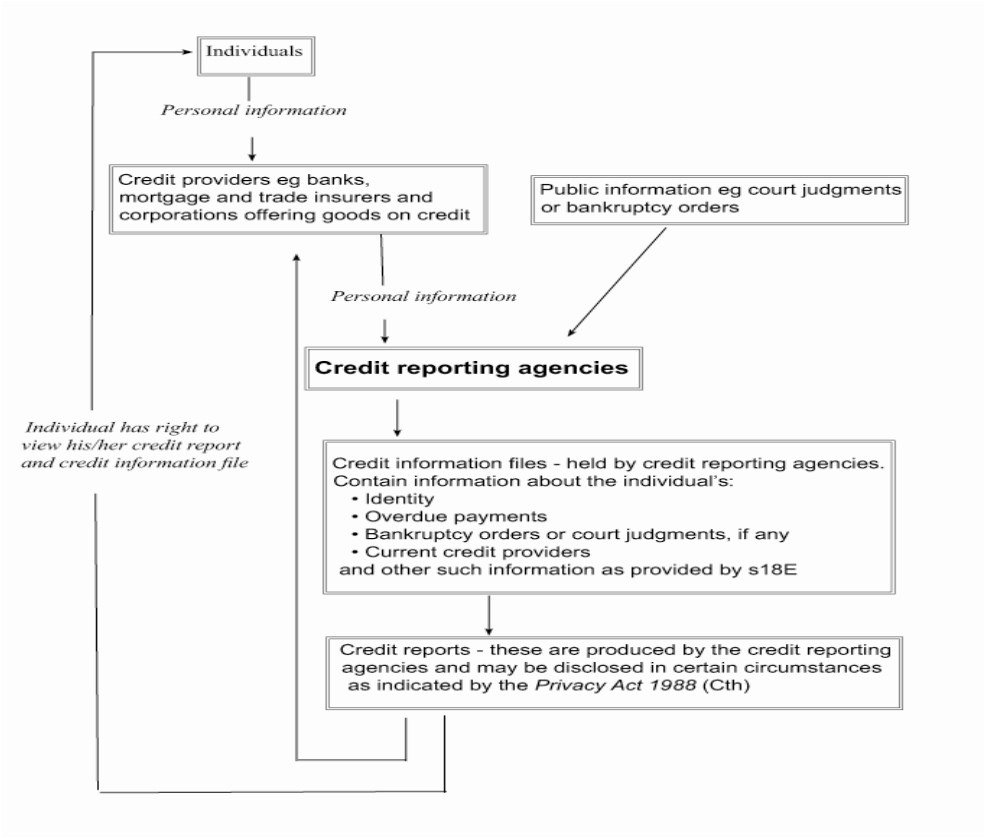
49.1 This chapter provides an overview of the credit reporting provisions of the *Privacy Act 1988* (Cth). Part IIIA of the *Privacy Act* contains the substantive provisions that regulate credit reporting. Some provisions dealing with the scope and application of the credit reporting provisions are located elsewhere in the Act. In addition, the Act empowers the Privacy Commissioner to issue a binding Code of Conduct.[1] A *Credit Reporting Code of Conduct* came into effect on 24 September 1991.

1 *Privacy Act 1988* (Cth) ss 18A, 18B.

49.2 The chapter first considers the people and information covered by the credit reporting provisions. It summarises how personal information may be used and disclosed in the credit reporting process, and how the Act provides for rights of access and correction for individuals in relation to their personal information. The chapter then considers the relationship between Part IIIA of the Act and the National Privacy Principles (NPPs).[2]

49.3 The chapter also describes the responsibilities and powers of the Office of the Privacy Commissioner (OPC) with regard to credit reporting[3] and the remedies and penalties in the event of non-compliance with the credit reporting provisions.[4]

49.4 Finally, this chapter sets out in detail how the *Privacy Act* permits and restricts the transfer of personal information in credit reporting. The diagram below is a summary of the main data flows under the present regulation of credit reporting.



2 The NPPs are located in Ibid sch 3.
3 The powers and responsibilities of the OPC generally are discussed in Part F.
4 The remedies and penalties available under the Act generally are also discussed in Part F.

Application of the credit reporting provisions

49.5 This part of the chapter answers the following questions. What information is covered by the credit reporting provisions? To whom do the provisions apply?

Information covered by the provisions

49.6 A number of terms define the scope of the regulatory framework for credit reporting in the *Privacy Act*. The most important of these are 'personal information', 'credit information file' and 'credit report'. Their respective meanings, and the inter-relationship of these terms, are discussed here.

49.7 The Act, principally in Part IIIA,[5] regulates the use and disclosure of 'personal information' for credit reporting purposes. 'Personal information' is defined to mean:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[6]

49.8 An individual's personal information may be collated by a credit reporting business to create a 'credit information file'. In relation to an individual, this means:

> any record that contains information relating to the individual and is kept by a credit reporting agency in the course of carrying on a credit reporting business (whether or not the record is a copy of the whole or part of, or was prepared using, a record kept by another credit reporting agency or any other person).[7]

49.9 The credit information file may in turn be used to create a 'credit report'. It is in this form that an individual's personal information may pass from the person collecting the information (the credit reporting agency) to the person wishing to use the information (the credit provider).[8] The term 'credit report' is defined as:

> any record or information, whether in a written, oral or other form, that:
>
> (a) is being or has been prepared by a credit reporting agency; and
>
> (b) has any bearing on an individual's:
>
> (i) eligibility to be provided with credit; or
>
> (ii) history in relation to credit; or
>
> (iii) capacity to repay credit; and

---

5 Note that other parts of the Act also relate to credit reporting. For instance, Part V deals with investigations by the Privacy Commissioner into alleged breaches of, among other things, the credit reporting rules.

6 *Privacy Act 1988* (Cth) s 6(1). The definition of 'personal information' is discussed in detail in Ch 3.

7 Ibid s 6(1).

8 The meanings of 'credit reporting agency' and 'credit provider' are discussed below.

> (c) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.[9]

49.10 Section 18N applies to a third category of personal information contained in 'reports', which term covers a much broader spectrum of documents than is encompassed by the term 'credit report'. Section 18N(9) states that 'report' means:

> (a) a credit report; or
>
> (b) subject to subsection (10), any other record or information, whether in a written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;
>
> but does not include a credit report or any other record or information in which the only personal information relating to individuals is publicly available information.

Persons within the ambit of the provisions

49.11 There are four main categories of person affected by Part IIIA of the *Privacy Act*. These are: (i) individuals; (ii) credit reporting agencies; (iii) credit providers; and (iv) third parties who provide personal information to credit reporting agencies.

Individuals

49.12 An individual, whose personal information forms the basis of a credit information file, may be affected by a credit report—especially in terms of the individual's application for credit. The Act stipulates that an individual must be 'a natural person' and that the definition of 'credit' does not include 'commercial credit'.[10]

49.13 This means that a corporation, for instance, cannot claim the protection of the credit reporting provisions in its own right. Commercial credit information is only indirectly regulated by the Act—where, for example, it is used to assess an application for consumer credit.[11]

Credit reporting agencies

49.14 The collection of personal information, its collation in credit information files and the disclosure of this information to credit providers only may be performed by a 'credit reporting agency'.[12] Section 11A provides that this term has two elements: a credit reporting agency must be a corporation and it must carry on a credit reporting business.

49.15 The requirement that a credit reporting agency must be a corporation is subject to a qualification. If the entity in question is engaged in wholly intra-state trade or

---

9 *Privacy Act 1988* (Cth) s 6(1).
10 Ibid s 6(1).
11 Ibid s 18L(4).
12 Ibid s 18C.

commerce, and it is not engaged in banking or insurance (other than state banking or state insurance), then it is not regulated by Part IIIA.[13]

49.16 Section 6(1) of the Act defines the second element of a credit reporting agency—namely, that the agency carry on a 'credit reporting business'—as being:

> a business or undertaking (other than a business or undertaking of a kind in respect of which regulations made for the purposes of subsection (5C) are in force) that involves the preparation or maintenance of records containing personal information relating to individuals (other than records in which the only personal information relating to individuals is publicly available information), for the purpose of, or for purposes that include as the dominant purpose the purpose of, providing to other persons (whether for profit or reward or otherwise) information on an individual's:
>
> (a) eligibility to be provided with credit; or
>
> (b) history in relation to credit; or
>
> (c) capacity to repay credit;
>
> whether or not the information is provided or intended to be provided for the purposes of assessing applications for credit.

49.17 This second element remains subject to some exemptions. Information concerning an individual's commercial transactions is excluded.[14] Also, the regulations may exempt certain businesses from being considered credit reporting businesses for the purposes of the Act.[15] To date, however, no such regulations have been made.

Credit providers

49.18 In general, credit reporting agencies may only disclose information in credit information files to 'credit providers'. Credit providers, in turn, may use credit reports only for certain purposes—notably, in assessing a person's application for credit.

49.19 There is a finite list of categories of entities considered credit providers for the purposes of Part IIIA. This list does not include, for instance, real estate agents, debt collectors, employers and general insurers, and thus they are not permitted to obtain credit reports.[16] Under the Act, the following are considered 'credit providers':

- a bank;[17]

---

13 See Ibid s 18C(2). This qualification is discussed in detail later in this chapter.

14 Ibid s 6(5A).

15 Ibid s 6(5C).

16 Office of the Privacy Commissioner, *Credit Reporting: Key Requirements of Part IIIA* <www.privacy.gov.au/act/credit/index.html> at 24 August 2007.

17 *Privacy Act 1988* (Cth) s 11B(1)(a). The term 'bank' is defined in s 6(1) to mean: (a) the Reserve Bank of Australia; or (b) a body corporate that is an authorised deposit-taking institution for the purposes of the *Banking Act 1959* (Cth); or (c) a person who carries on 'State banking' within the meaning of s 51(xiii) of the *Constitution*.

- a corporation, or an entity that is neither a corporation nor a government agency, that provides loans or issues credit cards as a substantial part of its business, or is carrying on a retail business;[18]

- an entity that provides loans (including by issuing credit cards), provided the Privacy Commissioner has made a determination in respect of such a class of entity;[19]

- a government agency that provides loans and is determined by the Privacy Commissioner to be a credit provider for the purposes of the Act;[20]

- a person who carries on a business involved in securitisation or managing loans that are subject to securitisation;[21] and

- an agent of a credit provider while the agent is carrying on a task necessary for the processing of a loan application, or managing a loan or account with the credit provider.[22]

49.20 The regulations also can exempt a corporation that would otherwise be considered a credit provider from being so regarded for the purposes of the Act.[23] To date, no such regulations have been made.

Persons providing personal information to credit reporting agencies

49.21 Finally, the credit reporting provisions also apply to a person, X, who provides personal information about another person, Y, to a third person, Z, carrying on a credit reporting business. Subject to certain constitutional limitations discussed later in this chapter, s 18D states that X must not give personal information about Y to Z unless Z is a corporation. Personal information is taken to be 'given' for the purposes of s 18D if the person to whom the information is given (ie, Z) 'is likely to use the information in the course of carrying on a credit reporting business'.[24]

Content of credit information files

49.22 A credit information file may contain information that is 'reasonably necessary … to identify the individual'.[25] Under s 18E(3), the Privacy Commissioner may determine 'the kinds of information that are … reasonably necessary to be included in

---

18 *Privacy Act 1988* (Cth) s 11B(1)(b), (c).
19 Ibid s 11B(1)(b)(v). These determinations are discussed further in Ch 50.
20 Ibid s 11B(1)(d). Indigenous Business Australia is the only entity deemed to be a credit provider under this provision: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.
21 *Privacy Act 1988* (Cth) s 11B(4A), (4B).
22 Ibid s 11B(5). The Act makes clear that 'the management of a loan' in subsection (5) does not include action taken to recover overdue loan repayments: s 11B(7).
23 Ibid s 11B(2).
24 Ibid s 18D(5).
25 Ibid s 18E(1)(a).

an individual's credit information file in order to identify the individual'. Any such determination is said to be a 'disallowable instrument', which means that it must be tabled in the Australian Parliament and is then subject to disallowance.[26] In 1991, the Privacy Commissioner determined that the following kinds of information are 'reasonably necessary' to identify the individual:

i. full name, including any known aliases; sex; and date of birth;

ii. a maximum of three addresses consisting of a current or last known address and two immediately previous addresses;

iii. name of current or last known employer; and

iv. driver's licence number.[27]

49.23 The Act does not state that information purporting to identify an individual must be verified in any particular way or be of any particular standard *before* it is included in a credit information file. This may be relevant to such issues as identity theft.

49.24 As well as information reasonably necessary to identify the individual, s 18E provides an exhaustive list of the other categories of personal information that may be included in a credit information file. Anything that constitutes personal information, but is not included in this list, may not be included in a credit information file. The Act allows a credit reporting agency to hold personal information in an individual's credit information file only for a finite period, the length of which depends on the nature of the information in question. After this period has elapsed, the agency must delete the relevant information within one month.[28]

49.25 In summary, information may be included in a credit information file if it is a record of:

- a credit provider having sought a credit report in connection with an application for consumer or commercial credit, provided the record also states the amount of credit sought;[29]

---

26 Ibid s 18E(4)–(6). Note that s 18E(6) of the *Privacy Act* refers to s 46A of the *Acts Interpretation Act 1901* (Cth). However, the latter provision has been repealed. Section 6(d)(i) of the *Legislative Instruments Act 2003* (Cth) provides that an instrument said to be a disallowable instrument for the purposes of s 46A of the *Acts Interpretation Act* should be considered a legislative instrument for the purposes of the *Legislative Instruments Act*.

27 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

28 *Privacy Act 1988* (Cth) s 18F(1).

29 Ibid s 18E(1)(b)(i). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

- a credit provider having sought a credit report for the purpose of assessing the risk in purchasing, or undertaking credit enhancement of, a loan by means of securitisation;[30]

- a mortgage or trade insurer having sought a credit report in connection with the provision of mortgage or trade insurance to a credit provider;[31]

- a credit provider having sought a credit report in connection with the individual having offered to act as guarantor for a loan;[32]

- a credit provider being a current credit provider in relation to the individual;[33]

- credit provided by a credit provider to an individual, where the individual is at least 60 days overdue in making a payment on that credit and the credit provider has taken steps to recover some or all of the credit outstanding;[34]

- a cheque for $100 or more that has been dishonoured twice;[35]

- a court judgment or bankruptcy order made against the individual;[36]

- a credit provider's opinion that the individual has committed a specific serious credit infringement;[37]

- an overdue payment to a credit provider by a person acting as guarantor to a borrower, provided the following conditions are met: the credit provider is not prevented by law from bringing proceedings to recover the overdue amount; the credit provider has given the guarantor notice of the borrower's default; 60 days have elapsed since the notice was given; and the credit provider has taken steps to recover the overdue payment from the guarantor;[38] and

---

30 Ibid s 18E(1)(b)(ia). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

31 Ibid s 18E(1)(b)(ii), (iii). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

32 Ibid s 18E(1)(b)(iv). The information may be kept for a maximum of five years after the relevant credit report was sought: s 18F(2)(a).

33 Ibid s 18E(1)(b)(v). The information may be kept for a maximum of 14 days after the credit reporting agency is notified that the credit provider is no longer the individual's credit provider: s 18F(2)(b).

34 Ibid s 18E(1)(b)(vi). The information may be kept for a maximum of five years after the credit reporting agency was informed of the overdue payment concerned: s 18F(2)(c).

35 Ibid s 18E(1)(b)(vii). The information may be kept for a maximum of five years after the second dishonouring of the cheque: s 18F(2)(d).

36 Ibid s 18E(1)(b)(viii), (ix). A record of judgment may be kept for a maximum of five years after the judgment was made: s 18F(2)(e). A record of a bankruptcy order may be kept for a maximum of seven years after the order was made: s 18F(2)(f).

37 Ibid s 18E(1)(b)(x). The information may be kept for a maximum of seven years after the information was included in the credit information file: s 18F(2)(g).

38 Ibid s 18E(1)(ba). The information may be kept for a maximum of five years after the credit reporting agency was informed of the overdue payment: s 18F(2A).

- a note or annotation to be made to an individual's existing credit information file, pursuant to ss 18J(2), 18F(4) or 18K(5).[39]

49.26 Certain types of personal information must never be included in an individual's credit information file. That is, information recording an individual's:

- political, social or religious beliefs or affiliations;
- criminal record;
- medical history or physical handicaps;
- race, ethnic origins or national origins;
- sexual preferences or practices; or
- lifestyle, character or reputation.[40]

49.27 If a credit report contains personal information that does not fall within the permitted categories, a credit provider who holds the report must not use this personal information, and must not use the report at all until the relevant information has been deleted.[41] A breach of this requirement constitutes a credit reporting infringement.[42] In this situation, an individual may complain to the Privacy Commissioner that the credit provider has committed an interference with the individual's privacy.[43] The Privacy Commissioner may then carry out an investigation and issue a determination in accordance with Part V of the Act.[44]

Accuracy and security of personal information

49.28 Credit reporting agencies and credit providers have obligations to ensure the accuracy and security of personal information in their possession or control. Credit reporting agencies and credit providers are required to take reasonable steps to ensure that:

---

39 Ibid s 18E(1)(c), (d); see also s 18E(7). Note that s 18J(2) obliges a credit reporting agency to include a statement of the correction, deletion or addition sought by an individual to his or her credit information file, where the agency has not made the relevant change; s 18F(4) requires a credit reporting agency, when appropriately informed, to include a note saying that the individual is no longer overdue in making a payment; and s 18K(5) requires a credit reporting agency to include a note on a person's credit information file when it has disclosed personal information from the file.

40 Ibid s 18E(2).

41 Ibid s 18L(3).

42 A breach of a provision of Part IIIA is a 'credit reporting infringement': Ibid s 6(1).

43 See Ibid ss 13(d), 36(1).

44 The Privacy Commissioner's complaint-handling processes are discussed in Ch 45.

- personal information in a file or report is 'accurate, up-to-date, complete and not misleading';

- the file or report is protected against 'misuse' including 'unauthorised access, use, modification or disclosure'; and

- if an agency or credit provider must give the file or report to a person in connection with the provision of a service to the agency or credit provider, it must 'prevent unauthorised use or disclosure of personal information contained in the file or report'.[45]

49.29 Credit reporting agencies and credit providers are prohibited from disclosing to anyone a false or misleading credit report. If an agency or provider intentionally contravenes this provision, it is liable for a fine of up to $75,000.[46]

Disclosure of personal information

49.30 The *Privacy Act* restricts how, and to whom, personal information in credit information files and credit reports may be disclosed. As explained below, the Act largely focuses on regulating the actions of credit reporting agencies, credit providers and others—setting rules on what these entities may do. Part IIIA, however, also prohibits any other person from obtaining access to a credit information file or credit report, where the Act does not authorise the person to do so, or where the person gains access by a false pretence.[47]

Credit reporting agencies

49.31 Section 18K of the Act contains four general rules on how personal information may be conveyed by credit reporting agencies to people who are permitted to view that information. If a credit reporting agency intentionally contravenes any of the relevant provisions, it is liable for a fine of up to $150,000.[48]

49.32 The general rules are as follows. First, a credit reporting agency is not permitted to make a credit information file directly available to another entity; instead the agency must convey that information in the form of a credit report. Secondly, a credit report only may be given to a credit provider.[49] Thirdly, personal information in a credit report only may be disclosed by a credit reporting agency for one of the purposes specified in the Act—these are summarised below. Fourthly, a credit reporting agency must not disclose personal information if the information does not fall within the permitted categories in s 18E, or if the agency is required to delete the information in

45 *Privacy Act 1988* (Cth) s 18G.
46 Ibid s 18R.
47 Ibid ss 18S, 18T. The penalty in respect of each offence is a fine not exceeding $30,000.
48 Ibid s 18K(5).
49 The terms 'credit report' and 'credit provider' are discussed earlier in this chapter.

question under s 18F.[50] These rules are, however, subject to certain exceptions, which are also set out below.

49.33 The purposes for which an individual's credit report may be given to a credit provider are set out exhaustively in the section. They relate to the state of mind and activities of the credit provider. The permitted purposes are to:

- assess the individual's application for credit;[51]
- assess the risk in purchasing, or undertaking credit enhancement of, a loan by means of securitisation;[52]
- assess an application for commercial credit, provided the individual agrees to the disclosure;[53]
- assess whether to accept the individual as a guarantor of a loan, provided the individual agrees in writing to the disclosure;[54]
- inform a current credit provider that the individual is at least 60 days overdue in making a payment to a second credit provider and this second credit provider has taken steps to recover some or all of the credit outstanding;[55]
- assist in collecting overdue payments from the individual;[56] and
- assist in collecting overdue payments in respect of commercial credit, provided the individual consents or the commercial credit was given prior to 24 September 1991.[57]

49.34 There are some situations in which a credit reporting agency may disclose an individual's credit report to a person who is not a credit provider, including disclosure to: (i) another credit reporting agency;[58] or (ii) a mortgage or trade insurer, where the insurer is assessing matters connected with whether to provide mortgage or trade insurance to a credit provider in respect of the individual.[59]

---

50 *Privacy Act 1988* (Cth) s 18K(2).
51 Ibid s 18K(1)(a).
52 Ibid s 18K(1)(ab), (ac).
53 Ibid s 18K(1)(b). The individual's agreement must usually be given in writing—see s 18K(1A).
54 Ibid s 18K(1)(c).
55 Ibid s 18K(1)(f). The relevant credit reporting agency is permitted to make such a disclosure only where it has received this information at least 30 days before the disclosure.
56 Ibid s 18K(1)(g).
57 Ibid s 18K(1)(h).
58 Ibid s 18K(1)(j).
59 Ibid s 18K(1)(d), (e). In respect of trade insurance, the disclosure is permitted only if the individual has agreed in writing: s 18K(1)(e).

49.35 The rule prohibiting the direct disclosure of personal information from an individual's credit information file is subject to a number of exceptions, namely where the:

- only personal information disclosed is publicly available;[60]
- disclosure is required or authorised by law;[61] or
- credit reporting agency is satisfied that a credit provider or law enforcement authority reasonably believes the individual has committed a serious credit infringement and the information is given to a credit provider or law enforcement authority.[62]

Credit providers

49.36 The rules dealing with how a credit provider may disclose personal information in its possession are set out in ss 18N and 18NA of the Act. The general rule is that a credit provider is prohibited from disclosing an individual's personal information (either from a credit report or other credit worthiness information held by the credit provider and that is not publicly available) unless a stated exception applies. If a credit provider intentionally contravenes this provision, it is liable for a fine of up to $150,000.[63]

49.37 There is a finite list of exceptions to the general rule. In summary, a credit provider is permitted to disclose an individual's personal information to:

- a credit reporting agency that is creating or modifying a credit information file;[64]
- another credit provider for a particular purpose, provided either the individual specifically agrees or it is in connection with an overdue payment;[65]
- the guarantor of an individual's loan in connection with enforcing the guarantee;[66]
- a mortgage insurer for the purpose of risk assessment or as required by the contract between the credit provider and the insurer;[67]

---

60 Ibid s 18K(1)(k).
61 Ibid s 18K(1)(m).
62 Ibid s 18K(1)(n).
63 Ibid s 18N(2).
64 Ibid s 18N(1)(a).
65 Ibid s 18N(1)(b), (fa).
66 Ibid s 18N(1)(ba).
67 Ibid s 18N(1)(bb).

- a recognised dispute settling body that is assisting in settling a dispute between the credit provider and the individual;[68]
- a government body with responsibility in this area;[69]
- a supplier of goods or services for the purpose of determining whether to accept a payment by credit card or funds transfer, provided the personal information disclosed does no more than identify the individual and inform the supplier whether the individual has sufficient funds for the proposed payment;[70]
- a person considering taking on the individual's debt, provided the personal information disclosed does no more than identify the individual and inform the person of the amount of the debt;[71]
- the guarantor, or a proposed guarantor, of a loan, provided the borrower specifically agrees;[72]
- a debt collector in respect of overdue payments to the credit provider, provided the personal information disclosed does no more than: identify the individual; give specified details relating to the debt; and provide a record of any adverse court judgments or bankruptcy orders;[73]
- a corporation related to the credit provider that is itself a corporation;[74]
- a corporation, in connection with its taking on a debt owed to the credit provider;[75]
- a person who manages loans made by the credit provider;[76]
- a person, as required or authorised by law;[77]

---

68 Ibid s 18N(1)(bc).
69 Ibid s 18N(1)(bd), (bda).
70 Ibid s 18N(1)(be).
71 Ibid s 18N(1)(bf).
72 Ibid s 18N(1)(bg), (bh). The borrower's agreement is not necessary if: the guarantee (or security) was provided before 7 December 1992; the information discloses the guarantor's liability; and the credit provider previously advised the borrower that such disclosures may take place: s 18N(1)(bg)(ii). See also s 18NA in respect of indemnities.
73 Ibid s 18N(1)(c). If the debt relates to commercial credit, the credit provider is prohibited from disclosing the details of the debt to a debt collector: s 18N(1)(ca).
74 Ibid s 18N(1)(d).
75 Ibid s 18N(1)(e).
76 Ibid s 18N(1)(f).
77 Ibid s 18N(1)(g).

- the individual or another person authorised by the individual;[78] and

- another credit provider or a law enforcement authority, where the credit provider reasonably suspects the individual has committed a serious credit infringement.[79]

49.38 The Privacy Commissioner has a power to determine the manner in which such a report may be disclosed;[80] however, the Commissioner is yet to make such a determination.

Information given by credit providers to credit reporting agencies

49.39 In practice, credit reporting agencies, in compiling credit information files, obtain most of that information from credit providers themselves.[81] This creates a two-way flow of personal information between credit reporting agencies and credit providers.

49.40 In view of this, the Act limits the information that a credit provider may provide to a credit reporting agency. That is, a credit provider must not give to a credit reporting agency personal information relating to an individual in any of the following situations:

- where the information would not fall within the categories in s 18E(1) summarised above;

- where the credit provider does not have reasonable grounds for believing the information is correct; or

- where the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency.[82]

Use of personal information

Credit providers

49.41 Section 18L(1) of the Act states the general rule that a credit provider may only use an individual's credit report, or personal information it derives from the credit report, for the purpose of assessing the individual's application for credit, or for one of the other permitted purposes for which the report was originally given to the credit

78 Ibid s 18N(1)(ga), (gb).
79 Ibid s 18N(1)(h).
80 Ibid s 18N(5)–(7).
81 This is specifically anticipated in Ibid ss 18E(8) and 18N(1)(a).
82 Ibid s 18E(8).

provider.[83] If a credit provider intentionally contravenes this provision, it is liable for a fine of up to $150,000.[84]

49.42 The rule in s 18L(1) is subject to the following exceptions, which allow a credit provider to use a credit report:

- as required or authorised by law;[85]
- if the credit provider reasonably believes the individual has committed a serious credit infringement, and the information is used in connection with the infringement;[86] or
- in connection with an individual's commercial activities or commercial credit worthiness, provided the individual agrees.[87]

Use and disclosure by mortgage and trade insurers

49.43 Mortgage and trade insurers must only use personal information contained in an individual's credit report in connection with assessing the risk in providing such insurance to the individual's credit provider, or as required or authorised by law.[88] They must not disclose personal information from a credit report to any person unless required or authorised by law.[89] If a mortgage or trade insurer 'knowingly or recklessly' contravenes any of these provisions, it is liable for a fine of up to $150,000.[90]

Use and disclosure by other persons

49.44 There are specific rules on how other persons may use personal information that they have obtained from a credit provider or credit reporting agency. Any person who intentionally contravenes one of these provisions will be liable for a fine of up to $30,000.[91] The rules are:

- Where a credit provider discloses information to a related corporation, the related corporation is subject to the use and disclosure limitations that apply to

---

83 The other permitted purposes are summarised earlier in this chapter.
84 *Privacy Act 1988* (Cth) s 18L(2).
85 Ibid s 18L(1)(e).
86 Ibid s 18L(1)(f).
87 Ibid s 18L(4), (4A). The Privacy Commissioner has a power to determine how this information may be used and how an individual's consent may be obtained: s 18L(6)–(8). To date, this power has not been exercised.
88 Ibid s 18P(1), (2). Mortgage insurers may also use such information pursuant to the contract between the mortgage insurer and the credit provider: s 18P(1)(c).
89 Ibid s 18P(5).
90 Ibid s 18P(6).
91 Ibid s 18Q(9).

the credit provider. The same rules also apply where a credit report is received by a person who was deemed to be a credit provider because it was engaged in securitisation of a loan, but has since ceased to be a credit provider.[92]

- Where information is received by a corporation, in connection with its taking on a debt owed to the credit provider, the corporation may only use the information in considering whether to take on the debt. If it takes on the debt, the corporation may use the information in connection with exercising its rights. Similar rules apply to a professional legal adviser or financial adviser in connection with advising the corporation about these matters, or as required or authorised by law.[93]

- Where information is received by a person who manages loans made by the credit provider, the information may only be used for managing these loans, or as required or authorised by law.[94]

Rights of access, correction and notification

49.45 Credit reporting agencies and credit providers, in possession or control of an individual's credit information file or credit report, must take reasonable steps to allow the individual access to the file or report. The individual can authorise another person (who is not a credit provider or a trade or mortgage insurer) to exercise these same rights in connection with applying for a loan, or advice in relation to a loan.[95]

49.46 Credit reporting agencies and credit providers must, in relation to credit information files and credit reports in their possession or control, 'take reasonable steps, by way of making appropriate corrections, deletions and additions, to ensure that personal information in the file or report is accurate, up-to-date, complete and not misleading'. If so requested, the agency or provider must either amend personal information in a file or report as requested by the individual concerned, or it must include a statement of the correction, deletion or addition sought by the individual.[96]

49.47 Credit providers also have notification obligations when they use a credit report to refuse an application for credit. Where a credit provider refuses an application for credit, and this refusal relates partly or wholly to information in an individual's credit report, the credit provider must: (i) notify the individual of these facts and of the individual's right to access his or her credit report; and (ii) provide the name and address of the relevant credit reporting agency.[97]

---

92 Ibid s 18Q(1), (6)–(7A).
93 Ibid s 18Q(2), (3). See also s 18Q(8).
94 Ibid s 18Q(4). See also s 18Q(8).
95 Ibid s 18H.
96 Ibid s 18J.
97 Ibid s 18M(1).

49.48 Where a joint application for credit is refused, and this refusal relates partly or wholly to information in the credit report of one of the applicants or proposed guarantors, the credit provider must inform the other applicants that the application was refused for this reason.[98] In this situation, however, the credit provider does not have to provide any further information, as the other applicants do not have a right to view the credit report of this person.

Responsibilities and powers of the OPC

49.49 The *Privacy Act* gives the OPC a range of responsibilities and powers under the Act.[99] These responsibilities and powers were described in more detail in Part F of this Discussion Paper. This chapter describes aspects of the OPC's responsibilities and powers in relation to:

- issuing a code of conduct relating to credit information files and credit reports;[100]
- making certain determinations, on the Privacy Commissioner's initiative, under the credit reporting provisions of the *Privacy Act*;[101]
- auditing credit information files and credit reports held by credit reporting agencies and credit providers;[102] and
- investigating credit reporting infringements,[103] either in response to a complaint or on the OPC's initiative,[104] and making determinations after investigating complaints.[105]

Credit Reporting Code of Conduct

49.50 Under s 18A of the *Privacy Act*, the Privacy Commissioner must, after consulting government, commercial, consumer and other relevant bodies,[106] issue a code of conduct concerning:

> (a) the collection of personal information for inclusion in individuals' credit information files; and

98 Ibid s 18M(2), (3).
99 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Ch 6.
100 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) issued under the *Privacy Act 1988* (Cth) s 18A.
101 *Privacy Act 1988* (Cth) ss 11B(1), 18E(3), 18K(3), 18L(6), 18N(5).
102 Ibid s 24A(1)(g).
103 A 'credit reporting infringement' is defined as a breach of either the *Credit Reporting Code of Conduct* or the provisions of pt IIIA: Ibid s 6.
104 Ibid pt V.
105 Ibid s 52.
106 Ibid s 18A(2).

> (b) the storage of, security of, access to, correction of, use of and disclosure of personal information included in individuals' credit information files or in credit reports; and
>
> (c) the manner in which credit reporting agencies and credit providers are to handle disputes relating to credit reporting; and
>
> (d) any other activities, engaged in by credit reporting agencies or credit providers, that are connected with credit reporting.[107]

49.51 In preparing the code of conduct, the Commissioner must have regard to the Information Privacy Principles (IPPs), the NPPs, Part IIIA of the Act and the likely costs to credit reporting agencies and credit providers of complying with the code.[108]

49.52 The *Credit Reporting Code of Conduct* (Code of Conduct) came into effect on 24 September 1991 and remains in force. The Code of Conduct is legally binding. Section 18B of the *Privacy Act* provides that a credit reporting agency or credit provider must not do an act, or engage in a practice, that breaches the Code of Conduct. Breach of the Code of Conduct constitutes a credit reporting infringement and an interference with privacy under s 13 of the Act.[109]

49.53 In broad terms, the Code of Conduct supplements Part IIIA on matters of detail not addressed by the Act. Among other things, the Code of Conduct requires credit providers and credit reporting agencies to:

- deal promptly with individual requests for access and amendment of personal credit information;
- ensure that only permitted and accurate information is included in an individual's credit information file;
- keep adequate records in regard to any disclosure of personal credit information;
- adopt specific procedures in settling credit reporting disputes; and
- provide staff training on the requirements of the *Privacy Act*.[110]

49.54 The Code of Conduct is accompanied by Explanatory Notes, which explain how Part IIIA and the Code interact. For example, in relation to the permitted content of credit information files, the Code of Conduct provides that:

> A credit reporting agency recording an enquiry made by a credit provider in connection with an application for credit may include, within the record of the enquiry, a general indication of the nature of the credit being sought.[111]

---

107 Ibid s 18A(1). The Code of Conduct is a disallowable instrument: *Privacy Act 1988* (Cth) s 18A(4).
108 *Privacy Act 1988* (Cth) s 18A(3).
109 Ibid s 13(d).
110 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), 3.
111 Ibid, [1.1].

49.55 The Explanatory Notes explain that, while s 18E(1) expressly permits inclusion of a record of an enquiry made by a credit provider in connection with an application for credit, together with the amount of credit sought:

> because of the size of the credit reporting system, and the large number and variety of credit applications recorded every year, it is accepted that an account type indicator should be allowed to be included in the file in order to facilitate speedy and accurate identification verification by credit providers of the enquiries recorded in credit information files.[112]

Determinations

49.56 The Privacy Commissioner has power to make certain determinations under the credit reporting provisions of the *Privacy Act*, including[113] determinations relating to:

- the definition of 'credit provider';[114] and
- the kinds of identifying information reasonably necessary to be included in credit information files.[115]

Credit provider determinations

49.57 Under Part IIIA, access to personal information provided by credit reporting agencies is generally restricted to businesses that are credit providers. Section 11B defines 'credit providers' for the purposes of the Act. In summary, under s 11B, financial organisations such as banks, building societies, credit unions and retail businesses that issue credit cards are automatically classed as credit providers.

49.58 Other businesses are also credit providers if they provide loans—defined to include arrangements under which a person receives goods or services with payment deferred, such as under a hire-purchase agreement[116]—and are included in a class of corporations determined by the Privacy Commissioner to be credit providers for the purpose of the Act.[117]

49.59 The Privacy Commissioner has made three determinations under s 11B of the Act. These include a determination that corporations are to be regarded as credit providers if they:

---

112 Ibid, Explanatory Notes, [1]–[2].

113 Other determinations by the Privacy Commissioner have been issued under *Privacy Act 1988* (Cth) s 18K(3)(b)—permitting the disclosure of certain information included in a credit information file or other record before the commencement of s 18K (24 September 1991).

114 Ibid s 11B(1).

115 Ibid s 18E(3).

116 Ibid s 6.

117 Ibid s 11B(1)(v)(B).

- make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least seven days; or

- engage in the hiring, leasing or renting of goods, where no amount, or an amount less than the value of the goods, is paid as deposit for return of the goods, and the relevant arrangement is one of at least seven days duration.[118]

49.60 Another determination deems corporations to be credit providers where they have acquired the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means).[119]

49.61 Both these determinations for privacy protection, in relation to the disclosure by credit reporting agencies of credit reports, are discussed further in Chapter 50.[120]

Identifying information

49.62 The Privacy Commissioner may determine the kinds of information that are, for the purposes of s 18E(1)(a), 'reasonably necessary to be included in an individual's credit information file in order to identify the individual'.[121] The Privacy Commissioner made a determination under this provision in 1991.[122]

Audits of credit information files

49.63 The Privacy Commissioner has power to audit credit information files and credit reports held by credit reporting agencies and credit providers.[123] The purpose of such audits is to ascertain whether credit information files and credit reports are being maintained in accordance with the Code of Conduct and Part IIIA of the *Privacy Act*.

49.64 The Privacy Commissioner also may examine the records of credit reporting agencies and credit providers to ensure that they are not using personal information in those records for unauthorised purposes, and are taking adequate steps to prevent unauthorised disclosure of those records.[124]

Investigating credit reporting infringements

49.65 Part V, Division 1 of the *Privacy Act* deals with the investigation of complaints and investigations on the Privacy Commissioner's initiative.[125] These provisions must

---

118 Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Providers)*, 21 August 2006.

119 Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

120 The third determination involves a specific corporation: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.

121 *Privacy Act 1988* (Cth) s 18E(3).

122 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

123 *Privacy Act 1988* (Cth) s 28A(1)(g).

124 Office of the Privacy Commissioner, *Credit Information Audit Process* <www.privacy.gov.au/publications> at 22 August 2007, 1.

125 These provisions are discussed in more detail in Ch 45.

be considered in association with the dispute settling procedures relating to credit reporting, which are set out in the Code of Conduct.

49.66 Under s 36(1) of the *Privacy Act* an individual may complain to the Privacy Commissioner about 'an act or practice that may be an interference with the privacy of the individual'. In the case of an act or practice engaged in by a credit reporting agency or credit provider, an act or practice is an interference with the privacy of an individual if it 'constitutes a credit reporting infringement in relation to personal information that relates to the individual'.[126] In turn, a 'credit reporting infringement' means a breach of the Code of Conduct or a breach of a provision of Part IIIA of the Act.[127] Subject to certain exceptions, the Privacy Commissioner must investigate an act or practice that may be an interference with the privacy of an individual if a complaint has been made under s 36.[128]

49.67 Under Division 2 of Part V of the *Privacy Act*, the Privacy Commissioner may make a determination after investigating a complaint. Under s 52, if the complaint is found to be substantiated, the determination may include declarations that the respondent not repeat or continue the conduct; or provide redress or compensation for any loss or damage suffered by the complainant.[129] The Privacy Commissioner may also order that a respondent make an appropriate correction, deletion or addition to a record, or attach to a record a statement provided by the complainant.[130]

49.68 Under s 41(2), the Privacy Commissioner may decide not to investigate, or to defer investigation, if satisfied that the respondent has dealt, or is dealing, adequately with the complaint; or if the respondent has not yet had an adequate opportunity to deal with the complaint.

49.69 The Code of Conduct sets out dispute settling procedures that must be followed by credit reporting agencies and credit providers.[131] The Code provides, among other things, that:

- credit reporting agencies and credit providers must handle credit reporting disputes in a fair, efficient and timely manner;[132]

- where a credit reporting agency establishes that it is unable to resolve a dispute it must immediately inform the individual concerned that it is unable to resolve

126 *Privacy Act 1988* (Cth) s 13(d).
127 Ibid s 6(1).
128 Ibid s 40(1).
129 Ibid s 52(1)(b).
130 Ibid s 52(3B).
131 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), pt 3.
132 Ibid, [3.1].

the dispute and that the individual may complain to the Privacy Commissioner;[133] and

- a credit provider should refer a dispute between that credit provider and an individual to a credit reporting agency for resolution where the dispute concerns the contents of a credit report issued by the credit reporting agency.[134]

Remedies and penalties

49.70 Part IIIA creates a range of credit reporting offences, including offences in relation to:

- non-corporations carrying on a credit reporting business;[135]
- persons giving personal information to a non-corporation carrying on a credit reporting business;[136]
- credit reporting agencies disclosing personal information other than as permitted;[137]
- credit providers using personal information contained in credit reports other than as permitted;[138]
- credit providers disclosing credit-worthiness information other than as permitted;[139]
- credit reporting agencies or credit providers intentionally giving out a credit report that contains false or misleading information;[140]
- persons intentionally obtaining unauthorised access to credit information files or credit reports;[141] and
- persons obtaining access to credit information files or credit reports by false pretences.[142]

133 Ibid, [3.2].
134 Ibid, [3.3].
135 *Privacy Act 1988* (Cth) s 18C(4).
136 Ibid s 18D(4).
137 Ibid s 18K(4).
138 Ibid s 18L(2).
139 Ibid s 18N(2).
140 Ibid s 18R(2).
141 Ibid s 18S(3).
142 Ibid s 18T.

50. The Approach to Reform

Contents

Introduction 1359
Part IIIA and the NPPs 1360
Options for reform 1362
Repeal and new regulation under the Act 1363
The anomalous nature of Part IIIA 1364
Duplication and complexity 1365
Specific credit reporting rules 1366
Sectoral credit reporting legislation 1366
Submissions and consultations 1367
ALRC's view 1371
Approaches to the new credit reporting regulations 1372
The regulations and the proposed UPPs 1372
Simplification of credit reporting regulation 1374
ALRC's view 1375
Application of the regulations 1377
Credit reporting information 1378
Credit reporting agencies 1380
Credit providers 1381
Application to foreign credit providers 1391
Consumer and commercial credit 1395
Credit reporting industry code 1398

Introduction

50.1 This chapter introduces the ALRC's proposals for reform of the credit reporting provisions of the *Privacy Act 1988* (Cth). The starting point for these proposals is the ALRC's preliminary view that Part IIIA and its related provisions should be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and the proposed Unified Privacy Principles (UPPs).[1] Under this proposed regime, privacy regulation specific to credit reporting would be set out in regulations promulgated under the Act.

1 The UPPs are discussed in Part D.

50.2 As discussed in this chapter, there are three main approaches available for reform of the credit reporting provisions:

- Credit reporting could continue to be regulated under Part IIIA of the *Privacy Act 1988* (Cth) and its related provisions.

- Part IIIA and its related provisions could be repealed, and credit reporting regulated under the general provisions of the *Privacy Act*.

- Credit reporting could be regulated by new sectoral legislation dealing specifically with the privacy of credit information files and credit reports.

50.3 There was little support in submissions for the retention of Part IIIA in its present form. As discussed in this chapter, even those who value the privacy protections provided by Part IIIA generally agree that the provisions should be simplified, while retaining the basic rules.

50.4 The ALRC proposes that the credit reporting provisions should be substantially rewritten in the form of regulations under the *Privacy Act*—referred to for the purposes of this Discussion Paper as the *Privacy (Credit Reporting Information) Regulations*. The reasons for this position are: the desirability of amending the Act to achieve greater logical consistency, simplicity and clarity, including by providing one set of overarching privacy principles (that is, the UPPs); and the need substantially to improve and amend the credit reporting provisions themselves—for example, to permit more comprehensive credit reporting[2] and to provide consumers with additional dispute resolution mechanisms.[3]

Part IIIA and the NPPs

50.5 In considering options for reform, it is important to understand the relationship between the credit reporting provisions of Part IIIA and the existing National Privacy Principles (NPPs).

50.6 Part IIIA of the *Privacy Act* was originally intended to adopt and reflect privacy principles in the specific context of credit reporting.[4] The NPPs were enacted later, in 2000,[5] and established a set of general principles designed to provide privacy protection in respect of personal information in the private (non-government) sector.

50.7 The rules in Part IIIA are designed to achieve broadly the same objectives as the NPPs. The obligations in Part IIIA apply only in respect of credit reporting whereas the

---

2 See Ch 51.
3 See Ch 55.
4 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).
5 *Privacy Amendment (Private Sector) Act 2000* (Cth). The NPPs are located in *Privacy Act 1988* (Cth) sch 3.

NPPs apply to the private sector generally. In substance, the provisions of Part IIIA of the *Privacy Act* constitute a third major set of privacy rules, in addition to the Information Privacy Principles (IPPs) and the NPPs—albeit more detailed and prescriptive than either of those sets of principles. For example, while NPP 1.1 sets out a general principle that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities, Part IIIA provides that a credit reporting agency must not include personal information in a credit information file unless the information comprises specified permitted content.[6]

50.8 The obligations in Part IIIA can be seen as both strengthening and derogating from the privacy protection afforded to personal information by the NPPs. A brief comparison of some of the NPPs and the credit reporting provisions illustrates this point.[7]

50.9 In some important respects, the NPPs can be seen as imposing a lower level of privacy protection than the provisions of Part IIIA:

- Under NPP 1, an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. This broad test of necessity can be contrasted with the detailed provisions of s 18E, which prescribe the permitted content of credit information files held by credit reporting agencies. Even if other categories of information can be shown to be necessary for credit reporting under NPP 1, collection is prohibited (even if the individual consents) under s 18E.

- Under NPP 2, an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless the secondary purpose is related or within the reasonable expectations of the individual concerned. In addition, NPP 2.1(c) permits, in some circumstances, the use of information for the secondary purpose of direct marketing—including by related bodies corporate.[8] In contrast, ss 18K and 18N limit the disclosure of personal information by credit reporting agencies and credit providers respectively to an exhaustive list of specific circumstances.

- Under NPP 3, an organisation must take reasonable steps to ensure that personal information it collects, uses or discloses is 'up-to-date'.[9] There is no equivalent of s 18F, however, which provides for the deletion of personal information in credit information files after the end of maximum permissible periods for the keeping of different kinds of information.

---

6 *Privacy Act 1988* (Cth) s 18E(1).
7 The proposed UPPs do not depart significantly from the NPPs in these respects.
8 *Privacy Act 1988* (Cth) s 13B.
9 A similar obligation applies to information in credit information files and credit reports: Ibid s 18G(a).

- Under NPP 6, individuals have rights to access to personal information about them. Unlike the equivalent rights under s 18H, NPP 6 specifically allows organisations to charge for access and contains an extensive list of exceptions, under which access may be refused in certain circumstances.

50.10 In other respects, the NPPs can be seen as imposing a higher level of privacy protection than the provisions of Part IIIA. Importantly, Part IIIA operates to authorise some information-handling practices that would not be permitted under the NPPs without the consent of the individual concerned:

- Sections 18K and 18N operate to authorise a range of secondary uses and disclosures of personal information that would not be permitted under NPP 2.1—for example, credit reports may be used by mortgage insurers and those considering entering securitisation arrangements, without the individual's consent.[10]

- The credit reporting provisions implicitly permit indirect collection of personal information by credit reporting agencies while NPP 1.4 requires that, if it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

50.11 A breach of a requirement of Part IIIA, unless the relevant provision states otherwise, has the same effect as a breach of one of the NPPs, and constitutes an 'interference with the privacy of an individual'.[11] Part IIIA and the NPPs operate independently.[12] Under s 13A(2), an organisation commits an interference with the privacy of an individual if it breaches a NPP, notwithstanding that the organisation is also a credit reporting agency or a credit provider. Section 16A(4) states that conduct that does not breach the NPPs is not lawful for the purposes of Part IIIA merely because it does not breach the NPPs.

Options for reform

50.12 In IP 32, the ALRC noted that review and reform of credit reporting regulation was generally favoured by consumer groups,[13] and that there was also active support within the financial sector for review, including in order to permit the introduction of more comprehensive credit reporting.[14] The credit reporting provisions may be criticised for being overly complex and prescriptive. Such is the complexity of the

10 Ibid ss 18K(1)(ab), (ac), and (d).
11 See Ibid s 13(d).
12 A Tyree, 'The Privacy (Private Sector) Amendments' (2000) 11 *Journal of Banking and Finance Law and Practice* 313, 315.
13 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).
14 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [7.35]–[7.40].

provisions, and the definitions in particular, that it has been suggested they should be rewritten even if the substance of regulation were to remain largely unchanged.

50.13 It has also been suggested that the credit reporting provisions operate as a barrier to new entrants into the credit reporting market and may hinder competition. The reasons for this view include that it takes a long period to develop databases of 'negative' events, such as defaults on loans; and complex and prescriptive legislative requirements increase the cost to a new entrant of developing the information technology infrastructure needed to conduct consumer credit reporting.

50.14 On the other hand, the credit reporting provisions were the result of significant parliamentary deliberation and may be viewed as having operated since 1991 without fundamental problems.

50.15 In IP 32, the ALRC asked whether Part IIIA, and related provisions of the *Privacy Act* dealing specifically with credit reporting, should:

- continue to regulate credit reporting, with appropriate amendment;
- be repealed, and credit reporting regulated under the *Privacy Act*, NPPs and a privacy code;
- be repealed, and credit reporting regulated under new sectoral legislation outside the *Privacy Act*; or
- be repealed, and credit reporting regulated by a self-regulatory scheme?[15]

Repeal and new regulation under the Act

50.16 The leading option for reform is to repeal the credit reporting provisions of the *Privacy Act* and leave credit reporting to be governed by the general provisions of the Act and the UPPs, supplemented by subordinate legislation. Some of the arguments in favour of this approach are discussed below, including the following:

- In dealing in detail with the handling of personal information within a particular industry or business sector, the credit reporting provisions are an unjustified anomaly within the *Privacy Act*. The Act would be significantly simplified by the repeal of Part IIIA.
- The independent operation of the NPPs and Part IIIA results in unnecessary duplication and complexity in the application of privacy principles. The repeal

15 Ibid, Question 7–1.

of Part IIIA is consistent with the ALRC's proposal to develop one set of privacy principles regulating both the public and private sectors.

- An equivalent level of privacy protection can be provided to individuals under the proposed new UPPs and a code or regulations dealing with credit reporting specifically.

The anomalous nature of Part IIIA

50.17 The credit reporting provisions are the only provisions in the *Privacy Act* that deal in detail with the handling of personal information within a particular industry or business sector. One credit reporting agency has observed that Part IIIA of the *Privacy Act* is a 'significantly more prescriptive legislative regime than applies to other arguably more sensitive sectors of the private sector'.[16] While it may be argued that credit reporting presents a suite of privacy issues that are uniquely deserving of specific regulation, the reasons for this anomaly are to some extent historical in that the credit reporting industry was made subject to privacy regulation before the rest of the private sector.

50.18 In 1990, when the credit reporting provisions were inserted into the *Privacy Act*, the Act had very limited application to the private sector.[17] While further privacy regulation was anticipated,[18] comprehensive coverage of the private sector was not implemented until 2000, with the enactment of the *Privacy Amendment (Private Sector) Act 2000* (Cth). The *Privacy Amendment (Private Sector) Act*, which came into effect on 21 December 2001, established the NPPs, which apply to the handling of personal information in the private sector.

50.19 The history of credit reporting regulation in Australia may be contrasted with that in New Zealand where credit reporting regulation, under a legally binding code, followed the enactment of the *Privacy Act 1993* (NZ), which applied information privacy principles across the public and private sectors.

50.20 As discussed in Chapter 15, the ALRC proposes that the IPPs and NPPs should be replaced by a single set of privacy principles regulating both the public and private sectors (the proposed UPPs). The repeal of Part IIIA is consistent with this proposal to develop one set of legislative privacy principles and with the approach taken to the privacy protection of health information.

---

16 Baycorp Advantage, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 16 March 2005.

17 The *Privacy Act* provided guidelines for the collection, handling and use of individual tax file number information in the private, as well as public, sector: *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).

18 For example, the second reading speech stated that the credit reporting provisions were 'the next step' in the Government's program to introduce comprehensive privacy protection: Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

Duplication and complexity

50.21 Arguably, the independent operation of the NPPs and Part IIIA results in unnecessary duplication and complexity in the application of privacy principles. First, there are overlapping rules where an organisation subject to the NPPs also falls within the ambit of Part IIIA.[19] When using personal information contained in a credit report, a bank, finance company or other credit provider must comply with both the NPPs and Part IIIA. On the other hand, the handling of other personal information relevant to credit worthiness by a credit provider, such as that obtained solely from the credit provider's own records, may be covered only by the NPPs.[20]

50.22 Other complexity results from the fact that Part IIIA distinguishes between consumer and commercial credit reporting. Part IIIA regulates consumer credit reporting activities, but does not cover personal information about commercial loans (that is, loans not intended to be used wholly or primarily for domestic, family or household purposes).[21] The handling of personal information relating to commercial loans is regulated primarily by the NPPs.

50.23 The regulation of publicly available information under the NPPs and Part IIIA is also complex. Under Part IIIA, the permitted content of credit information files includes some categories of publicly available information, notably information about court judgments and bankruptcy orders.[22] Some identifying particulars, such as an individual's current address, also may be publicly available. Other publicly available information is not regulated by Part IIIA, provided that it is kept separate from other information that affects credit worthiness.[23]

50.24 In contrast, the NPPs protect personal information that has been collected by an organisation and is held in a 'record'.[24] Personal information includes information that is publicly available, even if obtained from a generally available publication.[25]

---

19 Similarly, the obligations in pt IIIA may also overlap with those in the IPPs and tax file number provisions.

20 Note, however, that s 18N dealing with the disclosure of personal information protects a broader category of information than other provisions of pt IIIA, which protect information contained in a 'credit report' or 'credit information file'.

21 *Privacy Act 1988* (Cth) s 6(1) definition of 'credit'. However, pt IIIA touches on some aspects of commercial credit reporting. Section 18E(1)(b) permits credit reports to contain information about commercial credit and there are complex provisions to the effect that information about consumer credit can be used in commercial credit transactions, and vice versa, provided that agreement of the individual concerned is obtained: *Privacy Act 1988* (Cth) ss 18K(1)(b); 18L(4).

22 *Privacy Act 1988* (Cth) s 18E(1)(viii)–(ix).

23 See Ibid ss 6(1) (definition of 'credit reporting business'), 18K(1)(k), 18N(9).

24 Ibid s 16B. A 'record' is defined as a document, a database, or a photograph or other pictorial representation: *Privacy Act 1988* (Cth) s 6(1).

25 That is, while a 'record' does not include a 'generally available publication', a record may include personal information that is publicly available: *Privacy Act 1988* (Cth) s 6(1).

Separate records of publicly available personal information held by credit reporting agencies or credit providers, therefore, will be covered by the NPPs.

Specific credit reporting rules

50.25 The credit reporting provisions of the *Privacy Act* are complex and prescriptive. While some of this complexity and prescriptiveness may be unnecessary, effective regulation of credit reporting needs to incorporate at least some of this detail and, more generally, to tailor broad privacy principles to the specific conditions of the credit reporting industry. Incorporating the credit reporting provisions into regulations or a code under the *Privacy Act*, rather than leaving them in the primary legislation, makes it easier for rules to be amended to take into account the changing nature of the credit sector in Australia and developments in the role and potential uses of the credit reporting system.

50.26 One approach might be to incorporate the credit reporting provisions into a legally binding code issued by the Privacy Commissioner. Models of credit reporting privacy codes include those in New Zealand[26] and Hong Kong.[27] In New Zealand, credit reporting is regulated under a legally binding code issued by the Privacy Commissioner under the Act.[28] Many basic elements of the *Credit Reporting Privacy Code 2004* (NZ) are similar, in effect, to regulation in Australia.

Sectoral credit reporting legislation

50.27 An alternative approach to reform of the credit reporting provisions of the *Privacy Act* would be to repeal those provisions and enact new sectoral legislation dealing specifically with the privacy of credit reporting information.[29] In IP 32, the ALRC identified range of advantages and disadvantages of this approach.[30]

50.28 Some of the possible advantages were said to include that, given the detailed nature of credit reporting privacy regulation, it may be easier to regulate through sectoral legislation and that related, non-privacy consumer protection issues could be dealt with in legislation designed to operate consistently with the *Consumer Credit Code*.[31]

---

26 *Credit Reporting Privacy Code 2004* (NZ).

27 Office of the Privacy Commissioner for Personal Data Hong Kong, *Code of Practice on Consumer Credit Data* (1998).

28 *Credit Reporting Privacy Code 2004* (NZ) under *Privacy Act 1993* (NZ) s 46.

29 In this Discussion Paper, the term 'credit reporting information' is used to describe all personal information proposed to be covered by the *Privacy (Credit Reporting Information) Regulations*.

30 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [7.28]–[7.34].

31 The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.

50.29 The possible disadvantages include the following:

- Banks, finance companies and other credit providers would have to deal with two statutory privacy regimes—that is, specific rules in relation to credit reporting, and the proposed UPPs in relation to other aspects of handling personal information.

- Specific credit reporting legislation may add to problems caused by inconsistency and fragmentation in privacy law, including complexity of privacy regulation, varying levels of privacy protection, and regulatory gaps.[32]

50.30 The ALRC noted that, if credit reporting regulation were to be located outside the Act, questions may arise about whether the Privacy Commissioner remains the appropriate regulator.[33] For example, credit reporting conceivably could be regulated as a financial services consumer protection law by the Australian Securities and Investments Commission.

50.31 Overseas jurisdictions take differing approaches to the location of credit reporting legislation and the nature of the regulator. In the United States, credit reporting is regulated under the *Fair Credit Reporting Act 1970* (US) by the Federal Trade Commission.[34] In the United Kingdom, the activities of credit reference agencies are regulated by both the *Consumer Credit Act 1974* (UK) and under privacy legislation.[35] New Zealand and Canada more closely follow the Australian position. Credit reporting is regulated by these jurisdictions' privacy commissioners under the *Privacy Act 1993* (NZ) and the *Personal Information Protection and Electronic Documents Act 2000* (Canada) respectively.

Submissions and consultations

50.32 Stakeholders expressed a wide range of opinions on the approach to reform of the credit reporting provisions. These included views on whether Part IIIA should be repealed or retained, and on the regulatory model that might replace it.

---

32 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Ch 7.

33 The OPC already has some functions under legislation other than the *Privacy Act* including under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth); *National Health Act 1953* (Cth); *Telecommunications Act 1997* (Cth); and *Crimes Act 1914* (Cth): see Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006). IP 31 notes that one issue for consideration by the Inquiry is whether these functions should be consolidated under the *Privacy Act*.

34 Note that the United States does not have a federal information privacy commissioner.

35 The United Kingdom Information Commissioner (the equivalent of the OPC) deals with credit reporting complaints, and credit reference agencies are bound by the *Data Protection Act 1998* (UK).

50.33 A particular focus was on the respective roles in a regulatory model of the *Privacy Act* or new sectoral legislation, regulations or other subordinate legislation including legally binding codes, and self-regulation through industry codes.

Repeal of Part IIIA

50.34 There was explicit support in some submissions for the repeal of Part IIIA.[36] GE Capital Finance Australasia (GE Money), for example, stated:

> In our view, the benefits of adopting a principles-based approach to privacy regulation (including that flexibility required to deal with developing technologies and products over time) cannot be attained unless the provisions of Part IIIA of the Privacy Act are repealed.[37]

50.35 The Australian Finance Conference (AFC) stated that its preferred approach to reform would be 'the repeal of the current credit reporting provisions and regulation of consumer credit information under the NPPs and a Credit Reporting Code'.[38]

50.36 Other stakeholders called for a complete or substantial redrafting of Part IIIA.[39] Veda Advantage stated that the credit reporting provisions of Part IIIA are 'overly prescriptive and overly restrictive' and submitted that

> credit reporting regulation should be aligned with the National Privacy Principles (NPPs). Proceeding from a principle of proportionality, use and prevention of harm, we argue that the NPPs should apply to credit reporting, with additional protections applying to credit information in the hands of [credit reporting agencies] contained in a re-written Part IIIA.[40]

50.37 There was some support for the retention of Part IIIA, with modification. Abacus–Australian Mutuals stated that it supported the continued regulation of credit reporting within the scheme established under Part IIIA, but that 'it is timely for the ALRC to consider possible changes to the Part IIIA regime to refine and improve its application and effectiveness'.[41] In the view of the Consumer Action Law Centre, the existing credit reporting provisions are not 'in need of great change':

> While small improvements to the scheme could be made in various areas, the overall scheme is already relatively comprehensive and addresses key areas of concern. In our view, the main problems and concerns currently relate not to the rules, but to the way in which complaints handling and enforcement have operated in practice ...

---

36 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

37 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

38 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

39 Veda Advantage, *Submission PR 272,* 29 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007.

40 Veda Advantage, *Submission PR 272,* 29 March 2007.

41 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

> Improved avenues for dispute resolution and a greater emphasis on compliance and enforcement would be priorities.[42]

50.38 Optus stated that it believed the credit reporting provisions 'function well and do not require significant change'.

> In particular, to ensure the continuation of our ability to make informed and sound credit decisions, we oppose any moves to further restrict access to the data that is already available. Also, whilst we accept that the credit provisions could be simplified and re-worded, at this stage we are not supportive of any changes to the scope of the provisions.[43]

The regulatory model under the Privacy Act

50.39 The Consumer Action Law Centre considered that the various provisions of Part IIIA, the *Credit Reporting Code of Conduct* and the Privacy Commissioner's credit provider determinations[44] could be consolidated into 'one body of provisions, whether that be Part IIIA or a detailed code sitting under the National Privacy Principles'.[45]

50.40 The Centre was strongly opposed, however, to 'a reliance on the NPPs alone or to a self-regulatory system'.[46] Similarly, National Legal Aid supported the retention of 'separate provisions dealing with credit reporting rather than any proposal to collapse Part IIIA into the general provisions of the Privacy Act that deal with the private sector'.[47]

50.41 The Australian Privacy Foundation stated that it would be 'premature and dangerous' to change significantly either the location or the strength of the credit reporting provisions. The Foundation considered that prescriptive rules for credit reporting

> need not remain in a separate Part IIIA, but could instead be expressed as additional NPPs applying only to [credit reporting agencies] and/or [credit providers] as appropriate. Instead simplify the overall regulatory framework by consolidating the current mix of Part IIIA, Determinations and Code.[48]

50.42 Veda Advantage considered that, in addition to a rewritten Part IIIA, there should be credit reporting regulations, a code and a data governance standard.

> Regulations made under the Act should deal with what data cannot be collected, and who should have access to what level of data. A re-written Code would contain more

---

42 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.
43 Optus, *Submission PR 258,* 16 March 2007.
44 Under *Privacy Act 1988* (Cth) s 11B.
45 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.
46 Ibid.
47 National Legal Aid, *Submission PR 265,* 23 March 2007.
48 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

> detail preventing harmful uses of credit reporting data. Finally, [credit reporting agencies] would be required to be audited against a Data Governance Standard.[49]

50.43 The Office of the Privacy Commissioner (OPC) stated that Part IIIA should be repealed and credit reporting regulated under the NPPs and a binding code.

> The Office believes that this approach will provide a regulatory regime that is consistent with the principle based approach of the Privacy Act while at the same time imposing specific and enforceable obligations on credit providers and credit reporting agencies, in relation to their credit reporting activities.[50]

50.44 Other stakeholders favoured repeal of the prescriptive requirements of Part IIIA and submitted that credit reporting regulation should be reframed to reflect a principles-based approach.[51] GE Money, for example, stated that credit reporting should be regulated

> by privacy principles (including rules with legislative force developed in consultation with industry), in the way that the National Privacy Principles apply to other 'sensitive' information such as health related information.[52]

New sectoral legislation

50.45 There was little support expressed in submissions or consultations for new credit reporting legislation to be enacted outside the *Privacy Act*. One exception was the view, expressed by National Legal Aid, that ASIC, 'with a more comprehensive brief to monitor the finance and credit sectors', may be able to deal more effectively than the OPC with credit reporting issues that relate to broader systemic problems concerning the way credit is provided and debts are pursued.[53]

50.46 The OPC noted the difficulties that might be involved in regulating credit reporting as an industry matter rather than regulating the handling of personal information used in credit reporting. It stated that:

> significant dangers exist for creating further inconsistency and fragmentation in Australian privacy law through the implementation of sectoral legislation. This danger would increase with the number of different industry sectors in which credit reporting legislation was introduced.[54]

50.47 Veda Advantage noted that, internationally, credit reporting is regulated generally within privacy laws except where regulation of credit reporting preceded the

---

49 Veda Advantage, *Submission PR 272,* 29 March 2007.
50 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
51 Australian Finance Conference, *Submission PR 294,* 18 May 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007.
52 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.
53 National Legal Aid, *Submission PR 265,* 23 March 2007.
54 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

enactment of privacy laws, or where there is no comprehensive privacy or data protection legislation.[55] The Australian Privacy Foundation observed that

> the substance of credit reporting regulation is clearly fair information handling, which places it squarely in the area of data protection or information privacy law. On balance, we favour keeping the regulation of credit reporting within the *Privacy Act*, and urgently addressing the shortcomings of that Act and its enforcement.[56]

ALRC's view

50.48 The repeal of Part IIIA need not result in any lessening in privacy protection in relation to credit reporting. An equivalent level of privacy protection could be provided to individuals under the proposed UPPs supplemented by regulations or a legally binding code dealing with credit reporting issued by the Privacy Commissioner.

50.49 It is not would not be sufficient to leave credit reporting to be regulated by the UPPs alone, or by the UPPs supported only by some form of industry code. In comparison to general privacy principles (such as the existing NPPs or the proposed UPPs), the credit reporting provisions tend to a prescriptive rather than a principles-based regulatory approach. The ALRC agrees with the OPC, however, that

> credit reporting does require a certain of level of prescription to ensure that credit providers, credit reporting agencies and individuals understand their obligations and rights. Adverse personal credit listings can have a significant impact on the life and opportunities of an individual.[57]

50.50 This additional level of prescription should be provided by regulations promulgated under the *Privacy Act* rather than a code issued by the Privacy Commissioner.

50.51 The ALRC proposes, in Chapter 44, that Part IIIAA of the *Privacy Act* should be amended to empower the Privacy Commissioner to develop and impose a privacy code that applies to designated agencies and organisations.[58] Such codes would be unable, however, to impose less stringent requirements on agencies and organisations than are provided for in the UPPs. As discussed below, credit reporting regulations need to be able to impose more *or* less stringent requirements on credit reporting agencies and credit providers than provided for in the UPPs.

50.52 In any case, regulations are made by the Governor-General in Council, on the recommendation of the responsible minister (in this case, the Attorney-General). Even if the same result, in terms of privacy protection, might be achieved through a code,

---

55 Veda Advantage, *Submission PR 272,* 29 March 2007.

56 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

57 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

58 Proposal 44–10.

given the extensive consultation conducted by the ALRC, it seems more appropriate to recommend the promulgation of regulations than to leave matters for further consideration by the OPC. Proceeding by way of regulations also is consistent with the ALRC's approach to the privacy of health information.[59]

Proposal 50–1 The credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and proposed Unified Privacy Principles (UPPs).

Proposal 50–2 Privacy rules, which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be promulgated in regulations under the *Privacy Act*—the proposed *Privacy (Credit Reporting Information) Regulations*.

Approaches to the new credit reporting regulations

50.53 The following part of this chapter discusses a range of general issues relevant to the drafting of the proposed *Privacy (Credit Reporting Information) Regulations*. These include the relationship between the regulations and the proposed UPPs, and approaches to simplify the drafting of the regulations—at least as compared to the existing provisions of Part IIIA.

The regulations and the proposed UPPs

50.54 The content of the proposed *Privacy (Credit Reporting Information) Regulations* will include provisions that can be seen as both strengthening and derogating from the privacy protection afforded to personal information by the UPPs. For example, the *Privacy (Credit Reporting Information) Regulations* will continue to prescribe the permissible content of credit reporting information held by credit reporting agencies and will mandate the indirect collection of personal information.

50.55 The relationship between the UPPs and the *Privacy (Credit Reporting Information) Regulations* requires detailed consideration in light of the potential inconsistencies. Two broad approaches appear to be available.

50.56 The relationship between the UPPs and the *Privacy (Credit Reporting Information) Regulations* could mirror the existing relationship between the NPPs and Part IIIA of the *Privacy Act*. Credit reporting agencies and credit providers would have to comply with both regimes.

59 See Ch 56.

50.57 An alternative approach is taken in New Zealand under the *Credit Reporting Privacy Code 2004* (NZ) (NZ Code). The NZ Code is a binding code issued by the Privacy Commissioner pursuant to the *Privacy Act 1993* (NZ).[60]

50.58 The *Privacy Act 1993* (NZ) provides that the doing of any action that would otherwise be a breach of an information privacy principle[61] is deemed not to be a breach if the action is done in compliance with the NZ Code.[62] General requirements of the information privacy principles are incorporated into the credit reporting rules set out in the NZ Code, along with those that are different or more specific than provided for in the principles.

50.59 Some stakeholders addressed the possible relationship between new regulation of credit reporting and the obligations of organisations under the NPPs. The Australian Privacy Foundation and Nigel Waters of the Cyberspace Law and Policy Centre UNSW submitted that credit reporting regulation should not duplicate the obligations set out in general privacy principles.[63] The Foundation stated:

> where existing rules only duplicate obligations under the NPPs, they can be repealed, provided that all users of the credit reporting system are brought under the NPP regime, by removing them from the small business exemption.[64]

50.60 In this context, it should be noted that the ALRC proposes the *Privacy Act* be amended to remove the small business exemption by deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and repealing ss 6D–6EA of the Act.[65]

50.61 Waters submitted that a sensible approach to the review of the credit reporting provisions of the *Privacy Act* would be to 'map' the current regime, and any proposed changes, onto the 'foundation' NPPs.

> The NPPs, which are the default information privacy standard for all larger private sector businesses, cover the same ground as Part IIIA, the Code of Conduct, and the Credit Reporting Determinations, i.e. collection, data quality, transparency and notice, storage and retention, security, use, disclosure and access and correction. One objective of any reform should be to avoid simple repetition of NPP obligations in the

---

60 *Credit Reporting Privacy Code 2004* (NZ).

61 The information privacy principles are the NZ equivalent of the NPPs and IPPs.

62 *Privacy Act 1993* (NZ) s 53(a). On the other hand, failure to comply with the Code, even though that failure is not otherwise a breach of any information privacy principle, is deemed to be a breach of an information privacy principle: s 53(b).

63 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

64 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

65 Proposal 35–1.

> credit reporting 'rules'. Those rules should be confined to additional or more tailored obligations.[66]

50.62 Other stakeholders also commented on the relationship between Part IIIA and the NPPs. The Consumer Credit Legal Centre (NSW) (CCLC) submitted that:

> Part IIIA of the Act should be redrafted using the National Privacy Principles as a guide to the structure. Without diminishing the relevant rights and responsibilities of all parties, the obligations should be contained in a hierarchy under each privacy principle so that it is clear what each section or group of sections purport to achieve, and that the individual sections do not diminish the overarching obligation to observe the principle.[67]

50.63 Stakeholders considered that credit reporting regulation should align more closely with the obligations in the NPPs.[68] Veda Advantage stated, for example, that the credit reporting provisions 'fit poorly' with the principles based approach of the NPPs.

> The Act contains very detailed instructions and prohibitions on the use of data, while the NPPs are more 'broad brush' and principles-based. This leads to ambiguity and presents operational difficulties for business and consumers.[69]

Simplification of credit reporting regulation

50.64 Many stakeholders referred to the need to simplify credit reporting regulation.[70] The CCLC, for example, stated:

> The drafting of the current Part IIIA is complex, rigid and often difficult to comprehend and apply. It also arguably undermines the thrust of the privacy principles. Credit providers, consumers and decision-makers alike become mired in the detailed requirements of the Act and can easily lose sight of the principles those sections were meant to uphold.[71]

50.65 National Legal Aid observed that while some of the complexity of Part IIIA would have been difficult to avoid:[72]

> It is nevertheless worth asking whether there is now an opportunity to prune back some of this complexity, given the broader application of the *Privacy Act*, changes in

---

66 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

67 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007).

68 Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

69 Veda Advantage, *Submission PR 272,* 29 March 2007.

70 See, eg, N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Optus, *Submission PR 258,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007; AAPT Ltd, *Submission PR 87,* 15 January 2007.

71 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 67.

72 Given the need, among other things, to establish a firm constitutional basis for regulating consumer credit and avoid unforseen consequences to the finance industry of restricting access to credit reporting information: National Legal Aid, *Submission PR 265,* 23 March 2007.

> the way credit is provided and the enhanced capacity of computerised information systems.[73]

50.66 Industry stakeholders made similar comments. AAPT, for example, stated that the credit reporting provisions 'need to be re-written in plain English and in a simple style' and that the provisions are 'currently difficult to read and consumer protection must therefore be eroded'.[74]

ALRC's view

50.67 The ALRC considers that the existing credit reporting provisions contained in Part IIIA and associated provisions should be recast as regulations under the Act, incorporating content that reflects the policy recommendations resulting from the current Inquiry.

50.68 In drafting the *Privacy (Credit Reporting Information) Regulations,* the existing provisions of Part IIIA of the *Privacy Act* remain an appropriate starting point. Despite the criticisms made of the existing credit reporting provisions, Part IIIA of the Act provides comprehensive privacy protection. Further, the current practices of credit reporting agencies and credit providers have been developed to comply with these obligations. The AFC, for example, stated that:

> Significant resources have been expended to ensure documentation, procedures and training meet the requirements of Part IIIA and related provisions on an on-going basis … Any change would potentially impact and bring with it significant cost which may be borne by customers in the pricing of credit products.[75]

50.69 In the interests of maintaining privacy protection and minimising the transition costs to industry of new credit reporting regulations, any significant departure from the policy framework of Part IIIA needs to be justified.

50.70 The ALRC proposes, in Chapter 3, that the regulation-making power in the *Privacy Act* provide expressly that regulations may modify the operation of the UPPs to impose more or less stringent requirements.[76] Credit reporting agencies and credit providers should have to comply with both the UPPs and the *Privacy (Credit Reporting Information) Regulations*. This approach is consistent with the existing relationship between the credit reporting provisions and general privacy principles contained in the *Privacy Act*, and with the approach to be taken to the proposed *Privacy (Health Information) Regulations*.[77]

---

73 Ibid.
74 AAPT Ltd, *Submission PR 87,* 15 January 2007.
75 Australian Finance Conference, *Submission PR 294,* 18 May 2007.
76 See Proposal 3–1.
77 See Ch 56, Ch 15, Proposal 15–3.

50.71 The regulations should be drafted to contain only those requirements that are different or more specific than provided for in the UPPs. Any problems of inconsistency would be limited because conduct that complies with the *Privacy (Credit Reporting Information) Regulations* is 'required or authorised by law' under the UPPs.

50.72 There is potential for the *Privacy (Credit Reporting Information) Regulations* to simplify significantly the privacy rules relating to credit reporting. A number of approaches could be pursued. There is room, for example, to simplify the overall regulatory framework by consolidating the provisions of Part IIIA, the Privacy Commissioner determinations and the *Credit Reporting Code of Conduct*[78]—notably in relation to the definition of credit provider (discussed below).

50.73 In addition, some of the approaches taken in the NZ Code have the potential to simplify credit reporting regulation in Australia. The NZ Code is an important model because it was significantly influenced by the Australian credit reporting provisions and intended to bring about 'greater trans-Tasman regulatory alignment'.[79] Importantly, however, the New Zealand Privacy Commissioner also aimed to avoid some of the complexity and rigidity of Part IIIA.[80]

50.74 The New Zealand Assistant Privacy Commissioner has summarised the NZ Code as taking a similar approach to Part IIIA on some broad issues[81] and in some specific matters,[82] while being less complex and prescriptive.[83] There are, however, notable differences in some areas, including in relation to limits on the disclosure of credit information, which are less restrictive in New Zealand.[84]

50.75 One key approach taken under the NZ Code is to apply obligations to credit reporting agencies ('credit reporters') only and not credit providers. This can be contrasted with Part IIIA, which provides rights and obligations applicable to credit reporting agencies, credit providers and individuals.

50.76 The relative simplicity of the NZ Code approach can be illustrated by the differing approaches to the drafting of the provisions dealing with the use and disclosure of credit information. The NZ Code is able to deal succinctly with limits on use and disclosure of credit information by credit reporters in Rules 10 and 11

---

78 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

79 New Zealand Government Privacy Commissioner, *Credit Reporting Privacy Code: Frequently Asked Questions* (2006) <www.privacy.org.nz/privacy-act/frequently-asked-questions> at 31 July 2007.

80 B Stewart, 'Credit Reporting Privacy Code 2004' (Paper presented at New Zealand Credit & Finance Institute, Auckland, 21 February 2005).

81 For example, in relation to the information a credit reporting agency is permitted to collect.

82 For example, the definition of 'serious credit infringement'.

83 B Stewart, 'Credit Reporting Privacy Code 2004' (Paper presented at New Zealand Credit & Finance Institute, Auckland, 21 February 2005).

84 For example, a credit reporter may disclose credit information to a prospective landlord or employer: *Credit Reporting Privacy Code 2004* (NZ), Rule 11(2).

respectively, while Part IIIA of the *Privacy Act* relies on the extensive provisions of ss 18K, 18L, 18N, 18P and 18Q.[85]

50.77 Some of this simplicity results from that fact that, in New Zealand, the credit reporting activities of credit providers are regulated indirectly through obligations imposed under contract. Under the NZ Code, a credit reporter must ensure that a complying subscriber agreement is in place before disclosing any credit information to a credit provider.[86] There has been no call for such an approach in submissions.

50.78 More generally, the drafting and layout of the credit reporting provisions could be improved to assist credit providers, credit reporting agencies and consumers to understand their obligations and rights.[87] Many of the proposals made in this and subsequent chapters should contribute to a less complex form of credit reporting regulation.

50.79 It must be stressed, however, that it is not the ALRC's practice to draft regulations. As discussed in Chapter 1, this is partly because drafting is a specialised function better left to the legislative drafting experts and partly a recognition that the ALRC's time and resources are better directed towards determining the policy that will shape any resulting legislation.

Proposal 50–3 The obligations imposed on credit reporting agencies and credit providers by the proposed *Privacy (Credit Reporting Information) Regulations* should be in addition to those imposed by the proposed UPPs.

Proposal 50–4 The proposed *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the proposed UPPs.

Application of the regulations

50.80 A number of important issues arise in relation to the scope of the proposed regulations. As discussed in more detail in Chapter 49, the provisions of Part IIIA apply by reference to both the nature of the personal information and the person or

85 The NZ Code deals with the use and disclosure of credit information in less than 1,000 words, as compared to the 6,000 relevant words of Part IIIA (leaving aside related definitions).

86 See *Credit Reporting Privacy Code 2004* (NZ), Rules 5(2)(d); 8(3)(a); 11(2) and sch 3. The handling of credit information disclosed to a credit provider by a credit reporter is covered by the general information privacy principles of the *Privacy Act 1993* (NZ), as it would be if the information was obtained by the credit provider from its own clients directly.

87 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

organisation handling it. The following part of this chapter discusses issues arising in relation to the existing definitions of:

- 'credit information files', 'credit reports' and 'reports';
- 'credit reporting agency'; and
- 'credit provider'.

Credit reporting information

50.81 The provisions of Part IIIA apply variously to personal information in 'credit information files', 'credit reports' and 'reports'. As discussed in Chapter 49, each term is defined differently. Briefly:

- a credit information file is information kept by a credit reporting agency in the course of carrying on a credit reporting business;[88]
- a credit report is information prepared by a credit reporting agency that is used (by a credit provider) in establishing an individual's eligibility for credit;[89] and
- a report is a credit report or any other information that has any bearing on an individual's credit worthiness.[90]

50.82 Stakeholders have expressed support for reconsidering the retention of the separate terms, especially in view of commercial practice and technology.[91] Veda Advantage stated:

> For [credit reporting agencies] and their customers, the definitions of 'report', 'credit information' and 'credit report' are now out of step with commercial practice, technology and market demand, meaning that the information and business intelligence products we provide often have unclear or uncertain regulatory treatment, especially where they constitute a score, derived in part from information on a credit file.[92]

50.83 Veda Advantage submitted that the terms should be replaced with a single definition of 'credit information' based on the current definition of 'credit report'. Veda noted, however, that the use of 'data streams within the credit environment has meant that the traditional concept of a physical credit report no longer exists'.[93] An

---

88 *Privacy Act 1988* (Cth) s 6(1).
89 Ibid s 6(1).
90 Ibid s 18N(9).
91 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007.
92 Veda Advantage, *Submission PR 272,* 29 March 2007.
93 Ibid.

example is the development of automated credit card responses over the internet where a bank provides a '60 second response' in relation to a credit card application:

> The bank has a direct connection into the credit bureau and utilises elements of an individuals credit file to make the lending decision. There is no actual physical transfer or manual interrogation of a credit file—automated decision paths apply the banks assessment criteria. Credit data is more fluid, is used real time, and is an enabler of a larger process.[94]

50.84 The OPC stated that the usefulness of retaining these separate terms (especially the definition of a 'credit report') needs to be considered. Alternatively, the relationship between the terms needs to be defined with greater precision.[95] The Australian Privacy Foundation and Nigel Waters submitted that the ALRC should recognise the 'legitimate wider scope of the regime' recommending, that a new term, 'credit information', be introduced, defined in similar terms to a 'report' in s 18N(9).[96]

ALRC's view

50.85 The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'. The existing definitions of 'credit information files', 'credit reports' and 'reports' should not be reproduced in the new regulations.

50.86 The ALRC does not favour incorporating a broad definition of credit information based on the definition of 'report' in s 18N(9). As discussed in Chapter 53, the ALRC proposes that there should be no equivalent in the *Privacy (Credit Reporting Information) Regulations* of s 18N. Rather, the definition of credit reporting information should combine elements of the current definitions of 'credit information file' and 'credit report'.[97]

50.87 The ALRC suggests the following illustrative definition:

> ***credit reporting information***, means any record that contains personal information about an individual and is:
>
> (a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or
>
> (b) held by a credit provider and:

---

94 Ibid.
95 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
96 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.
97 *Privacy Act 1988* (Cth) s 6(1).

(i) is being or has been prepared by a credit reporting agency; and

(ii) has any bearing on an individual's eligibility to be provided with credit, history in relation to credit, or capacity to repay credit; and

(iii) is used, has been used or has the capacity to be used for the purpose of serving as a factor in establishing an individual's eligibility for credit.

Proposal 50–5 The proposed *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.

Credit reporting agencies

50.88 Under the *Privacy Act*, the term 'credit reporting agency' has the meaning given by s 11A. Briefly, a credit reporting agency is a corporation that carries on a 'credit reporting business'.

50.89 A 'credit reporting business' is defined as

> a business or undertaking … that involves the preparation or maintenance of records containing personal information relating to individuals (other than records in which the only personal information relating to individuals is publicly available information), for the purpose of, or for purposes that include as the dominant purpose the purpose of, providing to other persons (whether for profit or reward or otherwise) information on an individual's:
>
> (a) eligibility to be provided with credit; or
>
> (b) history in relation to credit; or
>
> (c) capacity to repay credit;
>
> whether or not the information is provided or intended to be provided for the purposes of assessing applications for credit.[98]

50.90 The OPC recommended that the definition of a 'credit reporting business' should be amended to remove the exclusion 'other than records in which the only personal information relating to individuals is publicly available information'.[99] This suggestion is consistent with the ALRC's proposal that the *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information (Proposal 52–6). The proposal below is intended to ensure that businesses that provide credit reporting information that is publicly available are caught by the regulations.

---

98 Ibid s 6(1).

99 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

Proposal 50–6 The definition of a 'credit reporting business' in the proposed *Privacy (Credit Reporting Information) Regulations*, if based on that in s 6(1) of the *Privacy Act*, should exclude the phrase 'other than records in which the only personal information relating to individuals is publicly available information'.

Credit providers

50.91 In general, credit reporting agencies may disclose personal information contained in credit information files (for example, a credit report) only to those persons who are 'credit providers' as that term is defined in the Act.[100] An entity is a credit provider under s 11B if the entity is, among other things,

- a bank;
- a corporation, a substantial part of whose business or undertaking is the provision of loans;
- a corporation that carries on a retail business in the course of which it issues credit cards; or
- a corporation that provides loans and is included in a class of corporations determined by the Privacy Commissioner to be credit providers for the purposes of the *Privacy Act*.[101]

50.92 A loan is defined to include a hire-purchase agreement or an agreement for the hiring, leasing or renting of goods or services under which full payment is not made or a full deposit is paid for the return of goods.[102]

Privacy Commissioner credit provider determinations

50.93 The Privacy Commissioner has made two determinations of general application[103] in relation to the definition of credit provider under s 11B. These determinations were renewed from August 2006.

---

100 These provisions are summarised in more detail in Ch 49.
101 *Privacy Act 1988* (Cth) s 11B(1)(b)(v)(B).
102 Ibid s 6(1), definition of 'loan'.
103 A third credit provider determination relates to a particular Australian Government agency and is not discussed here: Privacy Commissioner, *Credit Provider Determination No 2006–5 (Indigenous Business Australia)*, 25 October 2006.

50.94 Under the Privacy Commissioner's *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)* (Classes of Credit Provider Determination)—first made in substantially similar form in 1991—corporations are to be regarded as credit providers if they:

- make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least seven days; or

- engage in the hiring, leasing or renting of goods, where no amount, or an amount less than the value of the goods, is paid as deposit for return of the goods, and the relevant arrangement is one of at least seven days duration.[104]

50.95 Under the Privacy Commissioner's *Credit Provider Determination No. 2006–3 (Assignees)* (Assignees Determination)—first made in substantially similar form in 1995—corporations are to be regarded as credit providers for the purposes of the *Privacy Act* if they acquire the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means). A corporation deemed to be a credit provider by virtue of the Assignees Determination is regarded as the credit provider to whom the loan application was submitted, or who provided the loan.[105] The scope of these credit provider determinations raises a range of issues, which are discussed below.

50.96 Other issues concerning the definition of 'credit provider' include the fact that, under s 11B(1)(b)(iii), a corporation is a credit provider if a 'substantial' part of its business or undertaking is the provision of loans. This requirement may create uncertainty for corporations that provide loans as part of their business or undertaking. The OPC has stated that it considers that the word 'substantial' connotes both value and proportion—so that this aspect of the definition of a credit provider may be satisfied where a corporation's lending activities involve substantial amounts of money, even if such activities are not the dominant part of its overall business.[106]

Participation in the credit reporting system

50.97 The definition of credit provider raises broad issues about who should be permitted to participate in the credit reporting system; and what standards participants should have to comply with, in relation to credit reporting and more generally.

50.98 In IP 32, the ALRC noted, for example, suggestions that credit providers should have to comply with the *Consumer Credit Code* in order to participate in the credit

---

104 Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Providers)*, 21 August 2006.

105 Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

106 Office of the Privacy Commissioner, *Credit Reporting Advice Summaries* (2001), [1.4]. The OPC submitted that the definition of credit provider could be improved by defining the meaning of 'substantial' in legislation: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

reporting system.[107] The *Consumer Credit Code*, which has been adopted by all state and territory governments, governs many aspects of credit transactions and provides a range of important protections for consumers.

50.99 These protections include, for example, notice requirements that must be met before a credit provider may begin enforcement proceedings, prescribed periods within which a default may be remedied by the consumer,[108] and the power of a court to reopen an unjust transaction.[109]

50.100 Some organisations, which are recognised as credit providers for the purposes of the credit reporting provisions of the *Privacy Act*, are not required to comply with the *Consumer Credit Code*, which applies to 'credit providers' defined more narrowly.[110] Importantly, the *Consumer Credit Code* 'does not recognise services provided with payment in arrears terms as credit'.[111]

50.101 Other issues arise in relation to the classes of organisation that do not meet the current criteria for participation in the credit reporting system but consider that they should be permitted to obtain personal information contained in credit information files. Mercantile agents and others engaged in debt collection, investigation and related activities are one such group. Real estate agents and landlords are another. In relation to the latter, the NZ Code specifically permits a credit reporter to disclose credit information (where authorised by the individual) to a prospective landlord for the purpose of assessing the credit worthiness of the individual as a tenant.[112]

50.102 When considering what classes of persons or organisations should be permitted to obtain credit reports, it is important to understand that participation in the credit reporting system need not be 'all or nothing'. That is, regulation might permit different levels of access to the information contained in credit information files. For

---

107 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.97] referring to Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 15.

108 *Consumer Credit Code* ss 80–81.

109 In determining whether a transaction is unjust, the court may have regard to, among other things, whether 'the credit provider knew, or could have ascertained by reasonable inquiry of the debtor at the time, that the debtor could not pay': Ibid s 70(2)(l).

110 Under the *Consumer Credit Code*, a 'credit provider' is defined to mean a person who provides 'credit': Ibid s 3(1), Sch 1. For the purposes of the Code, credit is provided if, under a contract, 'payment of a debt … is deferred' or a person 'incurs a deferred debt to another': *Consumer Credit Code* s 4(1). The *Consumer Credit Code* applies only to the provision of credit where a charge is or may be made for providing the credit: *Consumer Credit Code* s 5(1).

111 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

112 *Credit Reporting Privacy Code 2004* (NZ) r 11(2)(b)(ii).

example, mercantile agents might be permitted to obtain name and address information in order to locate debtors, but not other details.[113]

Submissions and consultations

50.103 In IP 32, the ALRC noted concerns about the proliferation of entities that have access to the credit reporting system. Veda Advantage alone has over 5,000 subscribers.[114] The 2005 report of the Senate Legal and Constitutional References Committee's inquiry into the *Privacy Act* stated that:

> Determinations issued by the Privacy Commissioner under Part IIIA of the Privacy Act have extended access to the credit reporting system beyond traditional lenders such as banks to a wide range of retailers and service providers. Video store operators, legal services and healthcare providers, for example, are now deemed to be credit providers.[115]

50.104 In IP 32, the ALRC asked about the issues raised by the disclosure of personal information by credit reporting agencies to credit providers covered by the Privacy Commissioner's credit provider determinations, and by the definition of 'credit provider' more generally.[116]

50.105 Some stakeholders expressed concerns about the breadth of the definition of credit provider under the Privacy Commissioner's determinations.[117] National Legal Aid, for example, stated that while Part IIIA was intended to limit access to credit reporting information to 'genuine' credit providers, for the purpose of assessing credit worthiness, the definition of credit provider has led to

> determinations by the Privacy Commissioner that extend the definition to include sectors where the function of providing credit might be thought to be secondary to other activities. There are concerns that this has facilitated the process whereby credit reference services have become a resource for functions such as debt collection which the legislation was not designed to cover.[118]

---

113 This approach is currently taken in relation to disclosure of personal information by credit providers. Under s 18N(1)(c), a credit provider may disclose certain items of personal information to a debt collector from a credit report, but not others. The information that may be disclosed is limited to identifying information about the individual; information about overdue payments; and information about court judgments and bankruptcy orders.

114 Veda Advantage, *Submission PR 163,* 31 January 2007.

115 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.15]. The ALRC understands that, in practice, credit reporting agencies do not have any subscribers that are video store operators.

116 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 5–10 to 5–12.

117 Queensland Law Society, *Submission PR 286,* 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007. American Express favoured further restrictions if more comprehensive reporting is introduced: American Express, *Submission PR 257,* 16 March 2007.

118 National Legal Aid, *Submission PR 265,* 23 March 2007.

50.106 National Legal Aid expressed particular concern about the provisions of the Classes of Credit Provider Determination, which allows corporations to be regarded as credit providers if they provide goods or services on terms that allow the deferral of payment for at least seven days.

> The current definition is too broad. Few people would expect, or consider it reasonable, that their solicitor, dentist or builder should be able to access their personal credit information.[119]

50.107 The Assignees Determination was also criticised. National Legal Aid stated that assignees 'are typically debt collection agencies, which are thus given access to an information resource which was originally intended to exclude them from direct access to credit information files'.[120] In contrast, the AFC considered that the *Privacy Act* should be amended 'to specifically recognise assignees as credit providers in the relevant definition'.[121]

50.108 The Australian Privacy Foundation and Nigel Waters criticised the scope of the Privacy Commissioner's credit provider determinations and considered that the Commissioner had failed 'to strike the correct balance' between commercial interests and protecting the privacy of credit reporting information.

> We therefore submit that this power should be removed from the Commissioner, and that instead, the meaning of 'credit provider' should be exhaustively defined in the Act. Inadvertent oversight of legitimate claims … in the original legislation were rectified in early Determinations. These can now be incorporated in a new statutory definition. There has been enough experience of the law to ensure that all legitimate claims for inclusion have been brought to light and accommodated. Leaving the Commissioner with a power to further extend the definition is now just an open invitation for 'function creep'.[122]

50.109 This approach was echoed by the CCLC, which submitted that 'credit provider' should be clearly defined in the *Privacy Act* and that there should be 'capacity in the regulations to specifically exclude further categories of credit provider, but not to extend the definition'.[123]

---

119 Ibid.

120 The assignment or factoring of debts, including debts that are not overdue is, however, a common commercial practice: Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

121 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

122 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

123 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 35.

50.110 A number of stakeholders submitted that compliance with the *Consumer Credit Code* should be a condition of access to the credit reporting system.[124] The Banking and Financial Services Ombudsman (BFSO), for example, submitted that access should not be allowed unless the credit that has been provided is regulated credit, as defined in the *Consumer Credit Code*.

> This would also ensure that only those credit providers who are obliged to properly assess a consumer's capacity to repay a debt under the [*Consumer Credit Code*] are able to subsequently list a default with a credit reporting agency.[125]

50.111 The Consumer Action Law Centre shared concerns about access to credit reporting by 'non-traditional lenders':

> While the purpose of the credit reporting system is … to correct information asymmetry in the lending market, non-traditional 'lenders' such as utilities, medical practices and video stores primarily use the credit reporting system as a tool in debt collection and do not use the information at the time of deciding whether to provide services to a consumer on terms of payment in arrears (with the exception of some larger utility businesses).[126]

50.112 The Centre also noted that non-traditional lenders are more likely to be businesses that

> do not have the required dispute resolution systems in place … nor proper systems to ensure accurate data relating to the consumer and the debt (for example, whether it is statute-barred).[127]

50.113 The BFSO noted that regulation could permit some organisations that are not bound by the *Consumer Credit Code* (and are members of an external dispute resolution scheme) to obtain access to credit reporting information but not list defaults or serious credit infringements.[128] The Consumer Action Law Centre suggested that such a move would be consistent with the *Consumer Credit Code*, which does not provide consumers of services with the same level of protection as consumers taking out consumer credit.[129]

50.114 A particular focus of concern is access to the credit reporting system by telecommunications and utilities companies.[130] National Legal Aid stated:

---

124 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007. The OPC supported the 'alignment' of the definition of 'credit' in the *Privacy Act* with the definition in the *Consumer Credit Code*: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

125 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

126 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

127 Ibid.

128 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

129 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

130 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

> Legislation that was drafted with banks and building societies in mind, now applies to a broad range of 'credit providers'—most of the utilities—but does not adequately allow for billing disputes and other issues that arise with these 'credit providers'.[131]

50.115 Telecommunications and utilities companies use the credit reporting system to assess the credit worthiness of applicants for accounts and to assist in debt collection and may report overdue payments (defaults). The ALRC understands that telecommunications and utilities companies are credit providers for the purposes of Part IIIA of the *Privacy Act* by virtue of the Classes of Credit Provider Determination. These companies are not generally bound to comply with the provisions of the *Consumer Credit Code.*

50.116 The Telecommunications Industry Ombudsman stated that, in its view, the regulatory environment does not adequately reflect the role of telecommunications companies as credit providers for credit reporting purposes because

> at the 'front end' of the relationship between credit provider and consumer, there does not exist any like obligation on telecommunications providers to assess a consumer's capacity to pay for services which expose them to sizeable debt burdens, as there is for consumer credit providers regulated by the *Uniform Consumer Credit Code.* The inadequacy of assessment procedures in the telecommunications industry results in unacceptably large numbers of consumers incurring unexpectedly large debts which they have difficulty paying. This in turn exposes them to the risk of credit default listings.[132]

50.117 The CCLC recommended that telecommunications companies should be subject to 'similar regulatory obligations as consumer credit providers in relation to assessing ability to pay and/or providing appropriate products, dealing with financial hardship and notice prior to any form of enforcement action'.[133] The Australian Privacy Foundation submitted that the ALRC should 're-assess the arguments for and against inclusion of utility suppliers, and for special conditions and safeguards in relation to the use of credit reporting by utility suppliers'.[134]

50.118 On the other hand, telecommunications and utilities companies emphasised their need for credit reporting information. Optus noted that, without access to this information, it would be 'forced to undertake more intrusive information collection in order to assess the level of risk of providing that customer with a service'. Alternative credit assessment mechanisms, it was said,

---

131 National Legal Aid, *Submission PR 265,* 23 March 2007.
132 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.
133 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 24.
134 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

> could disadvantage some consumers who already find it difficult to pass a credit assessment, such as new migrants or young people moving out of home, making it more difficult for them to obtain telecommunications services.[135]

50.119 EnergyAustralia stated that it would be 'unfair to allow one particular class of credit provider access to information that enables them to make judgements about creditworthiness and deny this to another class of credit providers'. In particular, EnergyAustralia submitted that not all credit providers, for these purposes, should have to be covered by the *Consumer Credit Code*. The Code

> may conflict with acts and regulations under which specific industries operate. For example, electricity and gas industries have their own set of Acts and Regulations setting out what information must be included in a supply contract, requirements in relation to reminder notices, dispute resolution, marketing, disconnection of supply and security deposits among other matters.[136]

50.120 The ALRC notes that some steps have been taken to address concerns about credit management in telecommunications. In January 2006, following the identification of concerns that consumers may be at risk of unwittingly incurring high bills because they do not understand the costs, terms and conditions of telecommunications services,[137] the Australian Communications Industry Forum released a revised credit management code.[138] Most importantly for present purposes, the credit management code requires that certain procedures must be followed before reporting a customer to a credit reporting agency. For example, a supplier must take all reasonable steps to ensure that debts that are listed with a credit reporting agency do not include any unresolved service or billing issues involving disputed account balance amounts.[139]

50.121 Some stakeholders considered that, in some respects, the definition of credit provider is too restrictive and excludes some businesses that have legitimate claims to have access to credit reporting information. The AFC stated that the definition should be 'broadened to cover any business that supplies goods or services other than on an

---

135 Optus, *Submission PR 258,* 16 March 2007.

136 EnergyAustralia, *Submission PR 229,* 9 March 2007.

137 Australian Communications Authority, *Preventing Unexpectedly High Bills: Credit Management in Telecommunications* (2004).

138 Australian Communications Industry Forum, *Industry Code ACIF C541: 2006 Credit Management* (2006). The credit management code was registered by the Australian Communications and Media Authority on 13 April 2006 and binds telecommunications carriers and carriage service providers. The code deals with, among other things: the steps undertaken to enable a consumer to gain and maintain access to services; the minimum steps (including acceptable minimum timeframes for advising consumers) that a supplier must take before suspending, restricting or disconnecting a consumer's services; the processes that follow disconnection of services, including the collection of debts; and the disclosure of consumer personal information to a third party that may take place as a consequence of credit management action: Australian Communications Industry Forum, *Industry Code ACIF C541: 2006 Credit Management* (2006), i.

139 Australian Communications Industry Forum, *Industry Code ACIF C541: 2006 Credit Management* (2006), [5.10.2].

up-front cash basis' and the definition should not rely on any limit based on a fixed number of days for which payment is deferred:

> In our view, in order for the credit referencing system to have optimal value, it should be accessible by any business that supplies an individual with goods or services without requiring payment up-front (ie any business that provides a loan/gives credit).[140]

50.122 The AFC also submitted that real estate agents and employers should have regulated access to credit reporting information.[141] The Institute of Mercantile Agents stated:

> Currently, car hire firms and any business that uses credit cards as their main source of payment is denied the opportunity of using a credit reporting agency and the right to list a 'default' simply because under the current Act, they are not deemed a 'credit provider'. The current Act is fundamentally flawed in this aspect.[142]

ALRC's view

50.123 Submissions indicated a range of views, including those favouring new restrictions on access to the credit reporting system by excluding telecommunications and other service providers (or all organisations) that are not obliged to comply with the provisions of the uniform *Consumer Credit Code*.

50.124 There is room for different views on whether access to credit reporting information 'should be limited to businesses that are primarily credit providers, or whether the scheme should embrace all businesses that have a legitimate interest in knowing whether consumers represent a credit risk so that the way they collect and use credit related information can be appropriately regulated'.[143] The ALRC is not convinced that there is a sufficiently compelling case to tighten the definition of credit provider for the purpose of new credit reporting regulation.

50.125 The credit provider determinations have been in place since 1991 and commercial practices have developed in reliance on continued access to credit reporting information. The determinations were reviewed and renewed without substantive amendment by the OPC in 2006. The OPC concluded that while there were recurring issues that required attention, these issues had not prevented the Classes of Credit Provider Determination from operating satisfactorily.[144] The OPC undertook to develop information sheets and education strategies targeted at businesses covered by the Classes of Credit Provider Determination and those operating in the

---

140 Australian Finance Conference, *Submission PR 294,* 18 May 2007.
141 Ibid.
142 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.
143 National Legal Aid, *Submission PR 265,* 23 March 2007.
144 Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 20.

telecommunications sector; and to consider, as resources became available, the development of a credit reporting audit program focusing on non-traditional credit providers.[145]

50.126 Opponents of access by credit providers covered by the credit provider determinations did not deny that some of these businesses have an operational need for access to credit reporting information to assess the credit worthiness of potential customers. Objections to such access were based in large part on the use of default listing as a debt collection tool and on the quality of data reported by these credit providers.

50.127 Many of the concerns about the breadth of the definition of credit provider may be addressed effectively by the ALRC's proposals to improve credit reporting data quality (see Chapter 54) and complaint-handling procedures (Chapter 55). In particular, the ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where the credit provider is a member of an external dispute resolution (EDR) scheme approved by the OPC. This proposal is aimed at improving complaint-handling processes but may have the secondary effect of removing 'fringe' players from the credit reporting system who are unwilling to join an EDR scheme.

50.128 The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* should generally continue to be credit providers for the purposes of the new regulations.

50.129 The ALRC remains interested, nevertheless, in further comment on whether the new definition of credit provider could be tightened at the margins. One such option is to provide that organisations are to be regarded as credit providers if they make loans in respect of the provision of goods or services on terms that allow the deferral of payment for at least thirty days as compared to seven days, as is currently the case under the Classes of Credit Provider Determination. This would bring the definition into line with common trade terms relating to payment for invoiced goods or services.

50.130 A final issue concerns the drafting of the definition. Under the NZ Code, a credit provider is defined as an entity 'that carries on a business involving the provision of credit to an individual'. The term 'credit' means 'property or services acquired before payment, and money on loan'.[146] It has been suggested that the *Privacy (Credit*

---

145 Ibid, 22. The OPC also concluded that the Assignees Determination was operating satisfactorily and recommended that education programs should be developed and audit programs considered: Office of the Privacy Commissioner, *Report on the Review of the Credit Provider Determinations (Assignees and Classes of Credit Providers)* (2006), 20, 22.

146 *Credit Reporting Privacy Code 2004* (NZ) cl 5.

Reporting Information) Regulations should adopt a similar approach.[147] The ALRC is interested in further comment on this option, which (in contrast to the preceding suggestion) would loosen the definition of credit provider.

Proposal 50–7 The proposed *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* (whether by operation of s 11B of the *Privacy Act* or pursuant to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

Question 50–1 Should organisations be regarded as credit providers if they make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least thirty days as compared to seven days, as is currently the case under the OPC's *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)*?

Question 50–2 Should the definition of 'credit provider' under the *Credit Reporting Privacy Code 2004* (NZ) be adopted as the definition of 'credit provider' under the proposed *Privacy (Credit Reporting Information) Regulations*? That is, should 'credit provider' be defined simply as 'a person that carries on a business involving the provision of credit to an individual'; and credit as 'property or services acquired before payment, and money on loan'?

Application to foreign credit providers

50.131 In IP 32, the ALRC noted that there has been some concern about the: (a) listing on credit information files of information about foreign credit; and (b) disclosure of credit reports to foreign credit providers.[148] For example, as some credit reporting agencies operate in both New Zealand and Australia, individuals applying for credit in Australia may have default listings relating to loans from New Zealand credit providers.

50.132 Under the *Privacy Act*, a credit provider is defined to include a corporation if a substantial part of its business or undertaking is the provision of loans.[149] In turn, a

147 Veda Advantage, *Submission PR 272,* 29 March 2007.
148 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.163].
149 See *Privacy Act 1988* (Cth) s 11B.

corporation includes a foreign corporation within the meaning of s 51(xx) of the *Australian Constitution*.[150]

50.133 The provisions of s 5B of the *Privacy Act* dealing with its application to acts and practices outside Australia do not apply to the credit reporting provisions.[151] In particular, the Privacy Commissioner is not empowered to take action outside Australia to investigate credit reporting complaints.[152]

50.134 The OPC faces difficulties in investigating complaints about information from foreign credit providers, given limitations on the extraterritorial operation of Part IIIA. The ALRC understands that, in response to these concerns, Baycorp Advantage (now Veda Advantage) agreed not to include information about foreign loans in its credit reports.

50.135 More generally, there may be no means to ensure that a foreign credit provider complies with any of the obligations of credit providers under Part IIIA—for example, in relation to notifying individuals that information may be disclosed to a credit reporting agency.

50.136 In IP 32, the ALRC asked whether information from foreign credit providers or about foreign loans should be permitted in credit information files and credit reports; whether foreign credit providers should be permitted to obtain credit reports; and about issues of enforcement and the extraterritorial operation of the credit reporting provisions.[153]

50.137 The OPC confirmed that, based on the statutory construction of Part IIIA, it has taken the view that

> the listing of overseas incurred loans (and any information relating to those loans) on an individual's credit information file and the disclosure of personal information in credit information files … to a party overseas is not permitted by Part IIIA.[154]

50.138 In the OPC's view, practical and jurisdictional difficulties dictate that foreign credit providers and foreign loans should continue to be excluded from regulation under the *Privacy Act*. The Office suggested that the credit reporting provisions should explicitly exclude foreign credit providers.[155]

50.139 The CCLC stated that access by foreign credit providers would pose 'a huge risk of privacy abuse' and regulation could not be enforced effectively against them.[156]

---

150 Ibid s 6(1) definitions of 'corporation' and 'foreign corporation'.
151 Ibid s 5B(1).
152 Ibid s 5B(4).
153 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 5–27 and 5–28.
154 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
155 Ibid.
156 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

The Australian Privacy Foundation and Nigel Waters addressed the question of extraterritorial operation and submitted that there is no reason why the provisions of s 5B of the *Privacy Act* should not apply to Part IIIA.[157]

> Whatever application the Act has for private sector organisations subject to the NPPs, and the Commissioner's powers, should logically apply also to [credit reporting agencies and credit providers].[158]

50.140 Members of the Queensland Law Society stated that if foreign credit providers can demonstrate compliance with data security and complaint-handling procedures they should be permitted to access credit reporting information in Australia.[159] The Institute of Mercantile Agents also supported access by foreign credit providers.

> Our society is global and this global nature must be recognised in our credit reporting and privacy systems. Routinely, our industry sees consumers with default credit cards in multiple jurisdictions. Most OECD companies and many in Asia have similar privacy laws. Credit files should be transparent, especially if the credit applicant has signed an authority.[160]

50.141 Veda Advantage noted the desirability of facilitating transborder data flows of credit reporting information.

> A core issue for a company like Veda Advantage is the ability to deliver consumer data protection (keeping the promise that was originally made) when data is transferred across borders. Yet the globalisation of the credit business has created demand for accurate and complete historical credit data which encompasses all jurisdictions. The barriers to cross border data transfers impedes both credit providers and consumers from making the right decisions.[161]

50.142 Stakeholders focused specifically on the desirability of trans-Tasman flows of credit reporting information.[162] Dun and Bradstreet stated that, if consistency in credit reporting regulation is achieved, 'it should be permissible to list both Australian and New Zealand data on consumer credit reports in both countries'.[163]

50.143 Veda Advantage stated that it sought 'urgent measures' to 'permit trans-Tasman access to credit reporting for business and consumers'. Veda submitted that

---

157 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

158 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

159 Queensland Law Society, *Submission PR 286,* 20 April 2007.

160 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

161 Veda Advantage, *Submission PR 272,* 29 March 2007.

162 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007.

163 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

Australian and New Zealand credit providers should have 'limited access' to trans-Tasman credit reporting information and provide consumers with 'rights of access, correction, and notice'. In addition, regulators should provide guidelines to support these trans-Tasman rules, supported by an amendment to the extraterritoriality provisions of the *Privacy Act*.[164]

ALRC's view

50.144 Issues concerning the participation of foreign credit providers are linked to the regulation of transborder data flows, which is discussed in Chapter 28. The proposed 'Transborder Data Flows' principle is designed to regulate the transfer of Australian credit reporting information overseas, but has nothing to say about inward data flows—for example, a default report from an overseas credit provider that is transferred to an Australian credit reporting agency.

50.145 In theory, such a provision could be built into the proposed *Privacy (Credit Reporting Information) Regulations* so that, for example, foreign credit providers may report credit reporting information if they are subject to a law, binding scheme or contract which effectively upholds principles for fair handling of credit reporting information that are substantially similar to those in the proposed regulations. It is questionable, however, whether such a provision would work in practice.[165]

50.146 As discussed above, however, the primary concern about the reporting of personal information by overseas credit providers relates to the availability of effective enforcement and complaint handling. On this basis, the ALRC agrees with the OPC that foreign credit providers should, at least for the time being, be excluded from participation in the credit reporting system. The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should exclude the reporting of personal information about foreign credit and foreign credit providers; and the disclosure of credit reporting information to foreign credit providers.

50.147 In the future, however, it may be possible to facilitate credit reporting across jurisdictional boundaries and, in particular, between Australia and New Zealand. The Australian and New Zealand banking and financial services markets are highly integrated and many credit providers (and both major credit reporting agencies) operate on both sides of the Tasman. The New Zealand Privacy Commissioner observed, in this context, that 'consumer credit reporting is an activity in which the same major companies dominate business on both sides of the Tasman' and urged the ALRC to consider 'the trans-Tasman angle'.[166]

50.148 There are important benefits in maintaining harmonisation in the area of credit reporting, and harmonisation may ultimately permit integration of regulatory

---

164 Veda Advantage, *Submission PR 272,* 29 March 2007.
165 See Ch 28.
166 New Zealand Privacy Commissioner, *Submission PR 128,* 17 January 2007.

systems. Starting from their similar legal and commercial backgrounds, New Zealand and Australia have already achieved a significant degree of coordination and cooperation in a number of areas of business law (including in fair trading and other consumer protection law).

50.149 The countries are committed to further development of business law coordination under the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).[167] Recent progress in this regard has involved cross-border company recognition, cross-border insolvency provisions, mutual bans on disqualified company directors and information sharing between trans-Tasman competition and consumer regulators.[168] Coordinating the regulation of credit reporting regulation would be a subject consistent with this overall agenda.

Proposal 50–8 The proposed *Privacy (Credit Reporting Information) Regulations* should exclude: the reporting of personal information about foreign credit and foreign credit providers; and the disclosure of credit reporting information to foreign credit providers.

Proposal 50–9 The Australian Government should consider including credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).

Consumer and commercial credit

50.150 The credit reporting provisions are made more complex because Part IIIA distinguishes between consumer and commercial credit reporting. Part IIIA regulates consumer credit reporting activities, but does not cover personal information about commercial loans (that is, loans not intended to be used wholly or primarily for domestic, family or household purposes).[169] The handling of personal information relating to commercial loans is regulated primarily by the NPPs.

---

167 *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000) Department of Foreign Affairs and Trade <www.dfat.gov.au/geo/new_zealand/anz_cer/memorandum_of_understanding_business_law.html> at 1 August 2007.

168 P Costello (Australian Government Treasurer) and M Cullen (New Zealand Minister for Finance), 'Bilateral Progresses Single Economic Market Agenda' (Press Release, 29 January 2007).

169 *Privacy Act 1988* (Cth) s 6(1) definition of 'credit'.

50.151 Part IIIA, however, touches on some aspects of commercial credit reporting. For example, s 18E(1)(b) permits credit reports to contain information about commercial credit and there are complex provisions to the effect that information about consumer credit can be used in commercial credit transactions, and vice versa, provided that agreement of the individual concerned is obtained.[170] Further, the fact that an individual is the guarantor of a commercial loan is currently permitted content of a credit information file.[171]

50.152 In IP 32, the ALRC asked whether the distinction in the credit reporting provisions of the *Privacy Act* between consumer and commercial credit is necessary or whether personal information about consumer and commercial credit should be regulated by the same statutory provisions.[172]

50.153 Most stakeholders who addressed the issue in submissions favoured retaining the distinction between consumer and commercial credit reporting.[173] This view may be influenced, at least in part, by the fact that the *Consumer Credit Code* makes such a distinction.[174] From a consumer perspective, the CCLC stated:

> We contend in principle that commercial credit should be entitled to the same basic protections as consumer credit. In our view, it still remains a necessary distinction because in some matters we can envisage that consumer credit should have a higher level of protection.[175]

50.154 While industry stakeholders generally wanted commercial credit reporting to remain outside the rules set out in Part IIIA,[176] the Mortgage and Finance Association of Australia considered that the distinction between consumer and commercial credit was 'unnecessary and confusing'.[177]

50.155 The OPC noted that credit reporting agencies currently make an individual's commercial credit transactions available to credit providers to assess an individual's credit eligibility and that some provisions of Part IIIA already regulate aspects of

---

170 Ibid ss 18K(1)(b); 18L(4).

171 Under Ibid s 18E(1)(b)(iv), permitted content includes information in connection with an individual having offered to act as a guarantor in respect of a 'loan'. A 'loan', unlike 'credit', is not defined as being for 'domestic, family or household' purposes: *Privacy Act 1988* (Cth) s 6(1).

172 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–25.

173 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007. Some of these comments were premised on a misapprehension that regulation of credit reporting in respect of corporate entities was being contemplated.

174 *Consumer Credit Code* s 6(1)(b).

175 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

176 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007.

177 Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007.

commercial credit granted to individuals. This 'fragmented approach adds to the complexity of the provisions'.[178] The OPC recommended that personal information relating to credit advanced to an individual for commercial purposes should be covered by Part IIIA.[179]

ALRC's view

50.156 The current distinction between consumer and commercial credit may create needless complexity and appears inconsistent with the general approach of the *Privacy Act*. The *Privacy Act* does not distinguish in any other respect between personal information about an individual's personal and commercial activities. The distinction is not made in the NZ Code, which simply covers personal information that is credit information.

50.157 Where credit-related personal information is maintained by a credit reporting agency and is, for example, inaccurate or misleading, an individual should have the same rights of recourse regardless of whether the credit advanced was for a domestic or commercial purpose. The individual also should have the benefit of all the protections provided by the *Privacy (Credit Reporting Information) Regulations*.

50.158 This proposal does not mean that all credit-related information concerning an individual will be covered by the regulations (or the UPPs). The information must still be 'personal information'—that is, information 'about' an individual rather than, for example, about a company (of which the individual happens to be a director) having entered into a loan agreement.[180]

50.159 The ALRC remains interested, however, in further comments on the commercial implications of this proposal for credit reporting agencies and credit providers, for example, in view of the fact that the *Consumer Credit Code* does distinguish between consumer and other credit contracts.[181]

Proposal 50–10 The proposed *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit advanced to an individual for any purpose and not limited to 'domestic, family or household' purposes as is currently the case under the definition of 'credit' in the *Privacy Act*.

178 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
179 Ibid.
180 See, eg, *Durant v Financial Services Authority* [2003] EWCA Civ 1746.
181 See, Australian Finance Conference, *Submission PR 294,* 18 May 2007.

Credit reporting industry code

50.160 In this chapter, the ALRC proposes a model for new credit reporting regulation. Under this model, the credit reporting provisions of the *Privacy Act* would be repealed and credit reporting regulated under the general provisions of the Act and the proposed UPPs. Privacy rules imposing obligations on credit reporting agencies and credit providers specifically would be promulgated in regulations under the Act in the proposed *Privacy (Credit Reporting Information) Regulations*.

50.161 Some matters raised in the Inquiry, however, are not addressed most appropriately through legislation. For example, credit providers generally support the principle of reciprocity in credit reporting and obligations to report information consistently. Arguably, credit providers themselves and their industry associations should take responsibility for such matters, within the framework provided by legislation.

50.162 A desirable final element of the regulatory model is, therefore, a credit reporting industry code. Such a code should be developed by industry to deal with detailed operational matters—especially those relevant to compliance with data quality obligations—with input from consumer groups and regulators, including the OPC.

50.163 In Chapter 54, the ALRC proposes that the credit reporting industry code should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers (see Proposal 54–5). In Chapter 51, the ALRC proposes that the industry code should provide for access to information on credit information files according to principles of reciprocity (see Proposal 51–2).

50.164 The need for a self-regulatory code was reflected in comments made in submissions[182]—although in some cases, self-regulation was seen as substituting for, rather than augmenting, legislative regulation.

50.165 Experian referred to the United Kingdom regulatory model, which depends on a range of industry codes. Adherence to these codes is 'embedded in the agency contracts with their clients, thus any infringement would be likely to be a breach of contract and possibly a breach of the Data Protection Act'.[183]

50.166 Other stakeholders referred to the role of an industry code in regulating credit reporting. Dun and Bradstreet submitted that credit reporting should be regulated under the NPPs and an 'industry code of conduct'.[184] The industry group, the

182 See, eg, ANZ, *Submission PR 291,* 10 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

183 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

184 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

Australasian Retail Credit Association (ARCA), is developing an ARCA code of conduct that, it submits, should be used as 'the mandatory basis for credit reporting together with a strong link to the existing NPPs'.[185]

Proposal 50–11 Credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, an industry code dealing with operational matters such as default reporting obligations and protocols and procedures for the auditing of credit reporting information.

185 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

51. More Comprehensive Credit Reporting

Contents

Introduction 1401
'Positive' or 'more comprehensive' credit reporting? 1402
Australia's approach to more comprehensive credit reporting 1404
Current law 1404
Government responses 1405
The argument for more comprehensive credit reporting 1408
Benefits of more comprehensive credit reporting 1409
Improved risk assessment 1410
Promoting competition and efficiency 1412
Flow-on benefits for consumers 1413
Effects on the credit market and lending practices 1415
Problems with more comprehensive credit reporting 1418
Impact on privacy and security of personal data 1418
Empirical studies 1421
The limitations of empirical studies 1424
Veda Advantage research 1425
Regulation in other jurisdictions 1426
New Zealand 1426
United States 1427
United Kingdom 1427
Other jurisdictions 1428
Lessons for Australia 1428
Models of more comprehensive credit reporting 1429
New categories of personal information 1429
Reciprocity and reporting 1432
Type of credit reporting agency 1434
Privacy safeguards 1436
Should more comprehensive reporting be permitted? 1437
ALRC's view 1440

Introduction

51.1 This chapter considers proposals to extend the current system of credit reporting to permit a broader spectrum of personal information to be collected and disclosed—referred to in this Discussion Paper as 'more comprehensive' credit reporting.

51.2 This chapter begins by explaining what is meant by more comprehensive credit reporting and summarises the existing position with regard to the content of credit information files. The *Privacy Act 1988* (Cth), as explained in Chapter 49, restricts the types of personal information that may be collected and disclosed in the course of credit reporting. Broadly speaking, the Act mainly (but not exclusively) permits the collection and disclosure of personal information that detracts from an individual's credit worthiness—such as the fact that an individual has defaulted on a loan. This is commonly referred to as 'negative' or 'delinquency-based' credit reporting.

51.3 There has been a strong push by some stakeholders to expand the types of personal information that may be collected and disclosed in the credit reporting process. While these proposals differ in their detail, the common unifying feature is a system that permits the reporting of personal information relating to an individual's current credit commitments or repayment performance (or both).

51.4 This chapter examines the arguments for and against more comprehensive credit reporting, with particular reference to comments received in submissions and consultations, and information derived from empirical research into the possible effects of more comprehensive credit reporting on credit markets and the economy. The chapter also outlines some possible models of comprehensive credit reporting schemes, taking account of developments in other jurisdictions. For the reasons discussed in this chapter, the ALRC proposes that there should be a modest extension in the categories of personal information that may be collected for credit reporting purposes.

51.5 Any expansion in the categories of personal information that may be collected for credit reporting cannot be considered in isolation from other aspects of the privacy regulation of credit reporting —for example, in relation to the data quality of credit reporting information, dispute resolution and penalties for the unauthorised use or disclosure of such information. These and other issues are discussed in Chapters 52–55 of this Discussion Paper.

'Positive' or 'more comprehensive' credit reporting?

51.6 Much of the literature distinguishes between two distinct systems of credit reporting: 'negative' and 'positive' credit reporting.[1] The difference between these two sorts of credit reporting is said to lie in the kinds of personal information that can be collected as part of the credit reporting process. As the term suggests, negative credit reporting involves 'negative' information—that is, information that detracts from an individual's credit worthiness, such as the fact that an individual has defaulted on a loan. On the other hand, positive credit reporting is said to involve 'positive' information about an individual's credit position and includes information relating to

1 See, eg, Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

an individual's current credit commitments. An example of information in this category is a record of an individual having made a loan repayment.

51.7 The terms 'negative' and 'positive' credit reporting are sometimes used as convenient shorthand expressions to distinguish between what is permitted under the current law (negative reporting) and what may be permitted if the current restrictions on reporting were relaxed (positive reporting). The use of the terms in this way involves a significant over-simplification because the credit reporting provisions currently permit the collection of some 'positive' items.[2]

51.8 More fundamentally, the term 'positive credit reporting' may in fact be misleading because information collected through a positive credit reporting scheme can, in reality, be positive (in the sense of enhancing an individual's credit worthiness) or negative (that is, detracting from credit worthiness) depending on the particular situation. For example, 'data that is not default data can still be negative if it concerns missed payments or even very high levels of debt'.[3]

51.9 Therefore, a debate on whether 'positive' information should be included in credit reporting runs the risk of introducing a false premise—namely, that all information in this category would enhance the credit worthiness of the individual concerned. It is important that the debate be framed more clearly. As a result, the focus of this chapter is on whether it is appropriate to expand the categories of personal information involved in credit reporting and, if so, how.

51.10 Partly as a response to this semantic problem, some terms have been developed as alternatives to the term 'positive' credit reporting. The alternative term with the widest currency is 'comprehensive' credit reporting.[4] This term is preferable because it conveys more clearly that the information covered will not necessarily assist, nor hamper, an individual's application for credit. 'Comprehensive' in this context does not necessarily mean 'all' conceivable personal information of a financial nature that relates to an individual's credit worthiness. It is more appropriate, therefore, to talk about a *more comprehensive* system of credit reporting because this more accurately conveys the idea that what is being proposed is an expansion of the types of information a credit reporting agency can collect.

---

2 That is, a record of a credit provider being a current credit provider in relation to the individual: *Privacy Act 1988* (Cth) s 18E(1)(b)(v); a record of an enquiry made by a credit provider in connection with an application for credit, together with the amount of credit sought: s 18E(1)(b)(i).

3 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

4 See, eg, Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006). Another synonym is 'full-file reporting': see, eg, Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 1.

51.11 While the use of the term 'positive' credit reporting has become prevalent in describing proposals to expand credit reporting in Australia, the ALRC considers that 'comprehensive' or 'more comprehensive' credit reporting represent clearer and more accurate short-hand expressions. Therefore, when the terms 'comprehensive' or 'more comprehensive' credit reporting are used in this chapter, they simply refer to a system of credit reporting that permits more types of personal information to be collected and used in credit reporting than is currently allowed under the *Privacy Act*.

Australia's approach to more comprehensive credit reporting

51.12 There are many different models of more comprehensive credit reporting, as discussed below. However, most jurisdictions that permit some form of more comprehensive credit reporting include some or all of the following types of personal information:

- information about an individual's current loans or credit facilities, including the balances;
- an individual's repayment history;
- information about an individual's bank and other accounts, including the identity of the institution where the account is held and the number of accounts held; and
- further information than is currently permitted under the *Privacy Act* relating to overdue or defaulted payments.[5]

51.13 Reform to permit the collection and use of such categories of personal information in credit reporting would represent a significant extension of the current system.[6]

Current law

51.14 More comprehensive credit reporting is currently prohibited under the *Privacy Act*. This prohibition derives from the interaction of ss 18E and 18K.[7] Section 18E(1) sets out what information may be included in a credit information file.[8] The section provides that a credit reporting agency may include information that identifies the individual in question and sets out an exhaustive list of the other categories of personal information that may be included in the file. With some notable exceptions,[9] this list

---

5 See, eg, Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 2.

6 The personal information that may be used currently in credit reporting is summarised in Ch 49.

7 These provisions are summarised in greater detail in Ch 49.

8 In addition, *Privacy Act 1988* (Cth) s 18E(2) prohibits certain categories of personal information from being included in an individual's credit information file.

9 Ibid s 18E(1)(b)(v), s 18E(1)(b)(i).

contains mainly so-called negative information, such as information relating to the individual having defaulted on a loan.

51.15 Section 18K(2)(a) provides that a credit reporting agency must not disclose personal information if the information does not fall within the permitted categories in s 18E. Similarly, s 18E(8)(a) provides that a credit provider must not disclose personal information to a credit reporting agency if the information does not fall within the permitted categories in s 18E.

Government responses

51.16 Since the 1980s, both before and after the enactment of the credit reporting provisions, Australian federal and state governments have on several occasions had reason to consider the introduction of more comprehensive credit reporting.

Credit Reference Association of Australia proposal

51.17 As noted in Chapter 48, there was a push in the late 1980s for the introduction in Australia of a form of more comprehensive credit reporting. In that year, the Credit Reference Association of Australia (CRAA) stated its intention to collect information about individuals' current credit commitments.[10] This plan was postponed, however, at the request of the then Commonwealth Minister for Consumer Affairs, the Hon Nick Bolkus.[11] Subsequently, the Commonwealth Parliament passed the *Privacy Amendment Act 1990* (Cth), which had the effect of prohibiting 'positive' credit reporting.

51.18 There were a number of concerns about the CRAA's proposal. The New South Wales Privacy Committee feared that CRAA's proposal 'would greatly increase the quantity of personal information held by CRAA', and it may be too widely available.[12] The Australian Computer Society was concerned that this was 'an extremely privacy-invasive measure' demanding 'substantial justification'. It maintained that no detailed justification was publicly presented.[13]

51.19 Prior to the passage of the *Privacy Amendment Act 1990* (Cth), the then Minister for Consumer Affairs stated that one of the government's aims in passing this legislation was to 'tackle the whole question of positive reporting'. He noted that the government's rejection of 'positive reporting' was endorsed both by the Opposition and the Australian Democrats.[14] In the Second Reading Speech, the Minister went

---

10 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, [3.1].

11 New South Wales Government Privacy Committee, *Annual Report* (1989), 23.

12 Ibid, 22.

13 R Clarke, *Consumer Credit Reporting and Information Privacy Regulation* (1989) Australian Computer Society, [3.2].

14 Commonwealth, *Parliamentary Debates*, Senate, 15 August 1989, 13 (N Bolkus—Minister for Consumer Affairs).

further, stating that so-called 'positive reporting' represents an unwarranted 'intrusion into individuals' lives' and that:

> The Government does not consider that there is any proven substantial benefit from the positive reporting proposals and that in view of the strong privacy concerns held by the community this massive expansion of the extent of information held about individuals should not be allowed to develop.[15]

Financial System Inquiry (Wallis Report)

51.20 The Financial System Inquiry chaired by Mr Stan Wallis discussed the issue of more comprehensive credit reporting in its 1997 final report (the Wallis report).[16] The Wallis report stated that the inquiry was not in a position to assess whether the benefits of positive credit reporting outweighed the costs, but considered the potential benefits warranted a complete review of the issue.[17]

51.21 The Wallis report recommended that the Attorney-General should establish a working party, comprising representatives of consumer groups, privacy advocates, the financial services industry and credit reference associations to review the existing credit provisions of the *Privacy Act*. The purpose of this review should be to identify specific restrictions that prevent the adoption of world best practice techniques for credit assessment, and evaluate the economic loss associated with these restrictions against the extent to which privacy is impaired by their removal.[18]

Senate Legal and Constitutional References Committee

51.22 The inquiry undertaken in 2005 by the Commonwealth Senate Legal and Constitutional References Committee[19] (Senate Committee privacy inquiry) dealt with credit reporting. Generally, the inquiry stated that while 'government action is required to maintain community confidence in [the] integrity of the credit reporting regime', it did 'not see any need for review or reform of Part IIIA at this time'.[20]

51.23 Specifically, the Senate Committee privacy inquiry recommended 'that the Privacy Act not be amended to allow the introduction of positive credit reporting in Australia'.[21] It explained this position by saying:

> The committee sees no justification for the introduction of positive credit reporting in Australia. Moreover, the experience with the current range of credit information has shown that industry has not run the existing credit reporting system as well as would be expected and it is apparent that injustice can prevail. As mentioned elsewhere in this report, positive reporting is also rejected on the basis that it would magnify the

---

15 Commonwealth, *Parliamentary Debates*, Senate, 2 November 1989, 2788 (N Bolkus—Minister for Consumer Affairs).
16 Financial System Inquiry Committee, *Financial System Inquiry Final Report* (1997), 519–521.
17 Ibid, 521.
18 Ibid, rec 99.
19 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).
20 Ibid, [7.44]–[7.45].
21 Ibid, rec 17.

> problems associated [with] the accuracy and integrity of the current credit reporting system. The privacy and security risks associated with the existence of large private sector databases containing detailed information on millions of people are of major concern.[22]

51.24 The Australian Government disagreed with the Senate Committee's recommendation concerning credit reporting, stating that review of the credit reporting provisions is a matter that could be considered as part of the ALRC's current inquiry.[23]

Senate Economics Committee

51.25 The Senate Economics Committee also considered the issue in its 2005 report *Consenting Adults, Deficits and Household Debt: Links between Australia's Current Account Deficit, the Demand for Imported Goods and Household Debt*.[24] The Committee stated that it was not persuaded to take a different view to that expressed by the Senate Legal and Constitutional References Committee.

> The Committee does not believe that credit providers are making full use of the information currently available to them. Further … defaults and other signs of financial distress in the credit card market are very low and do not justify the very significant change that would be required for positive credit reporting to be introduced. The Committee does not consider that any further parliamentary inquiry into this matter is justified at this time.[25]

Victorian Consumer Credit Review

51.26 Finally, the 2006 Victorian Consumer Credit Review (the Victorian Review) dealt with comprehensive credit reporting as part of a broad review of the efficiency and fairness of the operation of credit markets and the regulation of credit in Victoria.[26]

51.27 The Victorian Review received a large number of submissions on the benefits and limitations of the current system of credit reporting, and in relation to proposals to institute more comprehensive credit reporting. Ultimately, it concluded that a form of more comprehensive credit reporting should not be introduced, at least 'while

---

22 Ibid, [7.46].

23 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006).

24 Parliament of Australia—Senate Economics Committee, *Consenting Adults, Deficits and Household Debt—Links Between Australia's Current Account Deficit, the Demand for Imported Goods and Household Debt* (2005), [5.61]–[5.87].

25 Ibid, [5.87]. Westpac observed that the Senate Committee 'found it difficult to understand what (if any) improvement adding additional information to credit bureaus would deliver': Westpac, *Submission PR 256,* 16 March 2007.

26 Victoria has its own legislation on credit reporting: *Credit Reporting Act 1978* (Vic). The Victorian Consumer Credit Review concluded that the Victorian legislation should be repealed because it has been superseded by the credit reporting provisions of the *Privacy Act 1988* (Cth): Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 280.

substantial questions remain about whether the benefits outweigh the costs', and it suggested further research and analysis in this area.[27]

51.28 In its response to the review, the Victorian Government agreed that comprehensive credit reporting should not now be implemented in Victoria on the ground that 'there is insufficient evidence' to show that it would be more beneficial than not to implement such a system. It went on to state that responsibility for '[f]urther research and analysis' in this area should be borne by the Commonwealth, as distinct from the Victorian Government.[28]

The argument for more comprehensive credit reporting

51.29 The *Privacy Act* contains strict limitations on the categories of personal information that may be collected and used as part of the credit reporting process. These have been criticised by those advocating the introduction of more comprehensive credit reporting in Australia.

51.30 The underlying basis for criticism of the current credit reporting regime is that it does not do enough to allow credit providers to redress the information asymmetry between the credit providers and potential borrowers.[29] As explained in Chapter 48, 'information asymmetry' refers to the situation where, because a credit provider often cannot know the full credit history of an individual applying for credit, the individual has more information about his or her credit risk than the credit provider. The greater the asymmetry, the harder it is for the credit provider to assess the risk premium associated with lending to the individual in question.[30]

51.31 The argument for reform of the current system of credit reporting is, in essence, that the current information asymmetry between credit providers and potential borrowers makes it unnecessarily difficult to assess the risk premium of individuals applying for credit. This, in turn, is said to cause a number of problems in assessing whether to provide credit. These were described in the Issues Paper, *Review of Privacy—Credit Reporting Provisions* (IP 32) as follows:[31]

- It is difficult for a credit provider accurately to assess the risk involved in lending to an individual. This paucity of information can cause the credit provider to 'select some bad borrowers' (who default in their repayments) and to

27 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 280.
28 Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 17.
29 See, eg, ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 13–14.
30 The 'risk premium' reflects the costs associated with lending to a potential borrower. See, eg, Ibid, 2.
31 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [6.28]–[6.29].

'ignore some good ones' (who would have made their repayments had credit been extended to them).[32]

- While 'good borrowers have no way of signalling their reliability' to credit providers, 'bad borrowers have no incentive' to disclose their lack of credit worthiness.[33]

- When an individual has committed 'a minor default in the previous five years [this] can prevent access to affordable and serviceable credit', even when the individual's circumstances have changed. For instance, a person who defaulted on a payment for his or her mobile phone when he or she was under the age of 18 may be refused credit at a later stage—after he or she has entered the workforce and consequently represents a much lower credit risk.[34]

51.32 Due to problems in assessing the risk presented by individual borrowers, credit providers may charge borrowers an average interest rate that takes account of their experience of the pool of borrowers (good and bad) to whom they lend. This may cause adverse selection so that 'some good borrowers to drop out of the credit market', further increasing the average interest rate 'to cover the cost of loans that are not repaid'.[35]

Benefits of more comprehensive credit reporting

51.33 In IP 32, the ALRC asked what are the advantages and disadvantages of more comprehensive credit reporting over the current credit reporting system and what would be the economic and social impact of introducing a system of more comprehensive credit reporting in Australia.[36]

51.34 There are a number of possible benefits that may result from introducing comprehensive credit reporting. Some of the possible benefits are discussed below with reference to views expressed in submissions.

---

32 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 2, 13–14.

33 Ibid, 14. See also Dun & Bradstreet, *Submission to Senate Economics Reference Committee Inquiry into Possible Links between Household Debt, Demand for Imported Goods and Australia's Current Account Deficit*, March 2005, 7.

34 Dun & Bradstreet, *Submission to Senate Economics Reference Committee Inquiry into Possible Links between Household Debt, Demand for Imported Goods and Australia's Current Account Deficit*, March 2005, 7.

35 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004); ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 17.

36 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 6–1, 6–2.

Improved risk assessment

51.35 The starting point for many of the purported benefits of more comprehensive credit reporting derive from the claim that it would improve the accuracy of credit risk assessment. The benefits said to flow from improved credit assessment include lower rates of over-indebtedness and default, greater competition in the credit market and less expensive credit. For example, it is said that the introduction of comprehensive credit reporting would increase the ability of credit providers to 'distinguish better between good and bad borrowers' and, in turn, reduce the rate of default and 'increase the volume of credit that can be provided to good borrowers'.[37]

51.36 Submissions from credit providers were virtually unanimous in the view that more comprehensive credit reporting has the potential to enhance credit risk assessment significantly.[38] As explained by Experian Asia Pacific (Experian):

> There is a general consensus amongst credit and risk professionals that the sharing of more information should lead to better decisions. When coupled with good regulatory protections for consumers the outcome is a robust and well balanced credit market.[39]

51.37 GE Capital Finance Australasia (GE Money) stated that:

> Our experience in a number of international markets is that comprehensive or 'positive' credit bureau data adds significantly to our ability to accurately assess an applicant's credit risk. This improved capability enables us to more accurately assess risk, which can in turn reduce credit losses (including fraud losses), a cost that is ultimately borne by consumers.[40]

51.38 Submissions contrasted the predictive power of the information currently available to that available under more comprehensive credit reporting systems. American Express submitted that inadequate data sharing under existing arrangements leads to problems of adverse selection and moral hazard.[41] In contrast, the application of more comprehensive information is able to 'detect those individuals comprising the pool of high risk potential debtors'.[42] Veda Advantage noted that:

> When overall levels of the borrower's obligations are provided as part of the 'positive data' then less reliance is needed on the incomplete data provided in negative only

---

37 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 19, 21. See also Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 7.

38 For example: Confidential, *Submission PR 297,* 1 June 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007; ANZ, *Submission PR 291,* 10 May 2007; Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

39 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

40 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

41 The meaning of these terms was discussed in Ch 48.

42 American Express, *Submission PR 257,* 16 March 2007.

> data environments. Lenders can then use the full picture of a consumers' indebtedness and their previous payment history to make a much more informed assessment of risk and hence a more responsible lending decision.

51.39 GE Money highlighted the predictive power of payment history information, as compared to information provided by an individual on an application form (and current credit reporting), when using credit risk scoring processes.

> Application demographic information such as 'time with current employer' and 'time at current address' are modelled based on how applicants with a similar profile (not the applicant individually) have performed in the past.
>
> An applicant's previous payment and spend behaviour data is by far the most predictive form of data because it is modelled on the actual performance of the applicant.
>
> The current credit bureau data only permits a credit provider to see one aspect (at the extreme end of the spectrum) of payment data, that is when someone has fallen into bankruptcy, had a default or serious credit infringement.[43]

51.40 GE Money stated that studies in a diverse range of international markets have proven 'aggregate account behaviour data' to add more predictive power to the credit scoring than the demographic data supplied by the applicant on the application form.[44]

51.41 Credit providers have legal obligations, including under the uniform *Consumer Credit Code* not to provide credit where capacity to repay has not been reasonably established. Submissions noted that more comprehensive credit reporting would enhance the ability of credit providers to comply with those obligations. For example, MasterCard Worldwide (MasterCard) stated:

> Greater availability of accurate data on an applicant's capacity to repay makes the UCCC a much [more] effective tool to prohibit over-extension, or impose sanctions on those [who] breach such prohibitions.[45]

51.42 MasterCard also submitted that consumer groups should, on that basis, lobby for the introduction of compulsory comprehensive credit reporting in Australia 'in much the same way that their counterparts in the United Kingdom are outspoken supporters of positive credit reporting there'.[46]

---

43 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

44 Ibid.

45 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

46 MasterCard claimed that many Australian debt counselling groups believe the system will reduce over-indebtedness: Ibid.

Promoting competition and efficiency

51.43 Comprehensive credit reporting is also said to promote competition in credit markets.[47] Among other things, more competition may mean that credit is more readily available, at lower cost, and in more forms than would otherwise be the case.

51.44 A report commissioned by MasterCard (the MasterCard/ACIL Tasman Report) stated that, for example, following increases in the types of personal data collected and used in credit reporting in the United States in the 1980s and 1990s, there was 'a wave of new entrants into the bank credit card market'. This led to 'downward pressure on interest rates and fees for bank credit cards' and 'the introduction of differential pricing in bank credit cards … with lower interest rate margins for lower risk borrowers', and an overall expansion in the credit card market.[48] In response, it may be observed that many of these developments also occurred in countries where there were no similar changes to credit reporting—including Australia.

51.45 In the Australian context, Abacus–Australian Mutuals (Abacus) noted that the ability of larger credit providers to use internal databases of 'positive' credit data relating to their own customers offers a potential competitive advantage in assessing credit risk. More comprehensive reporting may help create more competitive markets, because consumers are less reliant on existing institutional relationships to obtain credit.

> Those consumers with healthy repayment histories with one credit provider can, under a positive reporting scheme, transfer that good record to other credit providers. Under the current system, despite being able to demonstrate a capacity and propensity to repay, this positive data is not transferable within the credit reporting scheme.[49]

51.46 Other submissions referred to the promotion of more competitive credit markets.[50] For example, Dun and Bradstreet stated that 'improved data sharing is critical to the efficient operating of credit markets, resulting in improved products and rates for consumers and more efficient pricing for credit providers'.[51] Veda Advantage considered that more comprehensive reporting promotes competition in credit markets 'by reducing information barriers for small or new credit providers'.[52] GE Money stated:

---

47 See, eg, ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 23, 36.

48 Ibid, 31. There was a 'similar expansion' in mortgages and personal loans for motor vehicles: ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 32.

49 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

50 ANZ, *Submission PR 291,* 10 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

51 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

52 Veda Advantage, *Submission PR 272,* 29 March 2007.

> As demonstrated by the US and the UK experience when credit providers have the data that allows them to more accurately assess credit risk, entering into a new market segment becomes viable for providers who do not have existing customer bases.[53]

51.47 Submissions noted the possible role of more comprehensive credit reporting in reducing the transaction costs involved in assessing credit applications. For example, Experian considered that more comprehensive credit reporting could facilitate more automation and 'faster decisions' in credit and other financial services transactions.

51.48 The need for reform of credit reporting to maintain 'competitive neutrality' among credit providers was highlighted.[54] If more comprehensive credit reporting were introduced in Australia, this would also have a significant impact on the credit reporting market. For instance, it is said that this would enhance the capacity for competition between credit reporting agencies.[55] This should make it easier for relative newcomers in the Australian credit reporting market to increase their market share more rapidly.

51.49 Reference was made to the fact that the existing credit reporting provisions may operate as a barrier to new entrants into the credit reporting market and hinder competition.[56] The reasons for this view include that it takes a long period of time to develop databases of 'negative' events, such as defaults on loans; and complex and prescriptive legislative requirements increase the cost to a new entrant of developing the information technology infrastructure needed to conduct consumer credit reporting. The benefits of competition between credit reporting agencies might include improved data accuracy and a greater range of related services available to individuals and credit providers.[57]

Flow-on benefits for consumers

51.50 Improved risk assessment by credit providers and greater competition in credit markets may have a range of flow-on benefits for individual consumers in terms of lowering the cost of credit; increasing the availability of credit; reducing default rates; encouraging responsible lending practices; and promoting financial literacy.

51.51 Some argue that, by ensuring greater accuracy in risk assessment and management for credit providers, comprehensive credit reporting could help reduce the

---

53 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

54 MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

55 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 20. See, generally, ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 36.

56 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Law Council of Australia Privacy Working Group, *Consultation PC 32*, Sydney, 12 July 2006

57 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

cost of credit for individuals—particularly for those who are a low credit risk.[58] By allowing credit providers to assess risk more accurately, it would 'increase their scope to set interest rates to reflect the risk premiums associated with different types of borrowers'.[59]

51.52 In response to IP 32, a number of credit providers confirmed that more comprehensive credit reporting has the potential to lead to lower cost credit.[60] This outcome was attributed to the likely effects of increased competition between credit providers;[61] reduced credit provider costs associated with the risk assessment process;[62] and the reduced cost of bad debts.[63]

51.53 Another possible effect of more comprehensive reporting may be to increase access to credit, especially among low income earners.[64] Abacus noted that more comprehensive reporting may improve the chances of low income earners 'gaining access to mainstream credit and diminishing reliance on payday and other fringe lenders'.[65] Dun and Bradstreet submitted:

> The evidence demonstrates that comprehensive reporting allows improved access for under-served sections of the community to wealth creating credit such as home loans. This section of the community is often denied access to mainstream credit under a negative only system, due to an inability to demonstrate a strong payment history. Consequently they are forced into alternative credit arrangements often at hight rates of interest.[66]

51.54 American Express stated that more comprehensive reporting, by allowing credit providers to grant credit based on total debt exposure (and in the absence of proof of income), means that 'borrowers such as sole proprietors would have easier access to credit facilities'.[67]

---

58 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 11,* 13 April 2006, Annexure (Briefing Note), 4.

59 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 20.

60 American Express, *Submission PR 257,* 16 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

61 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

62 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 11,* 13 April 2006, Annexure (Briefing Note), 4.

63 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

64 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

65 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

66 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

67 American Express, *Submission PR 257,* 16 March 2007.

51.55 Submissions in support of more comprehensive credit reporting also focused on its possible role in reducing default rates and encouraging responsible lending practices.[68] At least in theory, a better understanding of a credit applicant's existing financial obligations should assist credit providers to avoid lending to those who are over-committed and to intervene to manage existing customers who become over-committed.

51.56 Some submissions also claimed that more comprehensive credit reporting will increase levels of 'financial literacy'[69]—the knowledge necessary for individuals to make informed decisions about the management of their personal finances. Arguably, individuals in jurisdictions that have systems that record 'positive' information about credit history are more aware of their 'credit rating' and the consequences of late payments or default. Individuals also have the potential to 'repair' their credit record after a default by subsequently establishing a solid repayment history.[70] In Australia, by comparison, many individuals are not even aware of the credit reporting system unless they have actually been refused credit as a result of information in their credit information file.

Effects on the credit market and lending practices

51.57 One of the claimed benefits of more comprehensive credit reporting is that it can reduce levels of over-indebtedness and default because credit providers will be in a better position to gauge when credit should be refused. However, some have challenged this proposition.

51.58 In response to the claimed link between the categories of personal information available to credit providers and overall levels of indebtedness, the Victorian Review cited research carried out in 2003 by Nicola Jentzsch and Amparo San José Riestra. This research found that evidence from the European and United States markets 'does not support the argument that there is a relationship between [the existence of comprehensive credit reporting] and lower levels of indebtedness'.[71]

51.59 The Victorian Review suggested that, if this conclusion is correct, it throws into doubt whether 'more information in a credit report' can 'assist in managing risk' or aid

---

68 Veda Advantage, *Submission PR 272,* 29 March 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

69 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

70 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

71 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 274, citing N Jentzsch and A San José Riestra, *Information Sharing and Its Implications for Consumer Credit Markets: United States vs Europe* (2003) European University Institute <www.iue.it/FinConsEU/ResearchActivities/EconomicsOfConsumerCreditMay2003> at 1 August 2007, 13.

'responsible lending'.[72] The Consumers' Federation of Australia (CFA) has also argued that, rather than comprehensive credit reporting decreasing the number of individuals defaulting on repayments, it is 'likely to increase the number of consumer credit defaults'.[73]

51.60 The CFA maintained that research conducted by United States economists Professors John Barron and Michael Staten (the Barron and Staten research), relied on by a number of the advocates of comprehensive credit reporting, is equivocal on this point.[74] The CFA stated that the conclusion of Barron and Staten's research is that comprehensive credit reporting could result in either greater availability of credit (with the current rate of default) or a lower rate of default (with a correspondingly lower availability of credit), but not both. It argued that the two results cannot be achieved simultaneously and 'the most likely outcome is more lending, rather than reduced defaults'.[75]

51.61 This interpretation was restated in submissions to the Inquiry by consumer groups.[76] The Consumer Action Law Centre stated that the actual outcome of more comprehensive reporting will depend on whether credit providers choose to reduce default rates or to advance more credit.

> Given that the latter allows for more lending business overall, it is highly likely that [comprehensive credit reporting] would mean lenders choose to expand their businesses. While the default rate would remain the same, the greater overall business means that more people overall would face defaults, and in human terms defaults equate to financial hardship, home losses, impaired credit information files and bankruptcies.[77]

51.62 MasterCard submitted that it is a misinterpretation of the Barron and Staten research to suggest that more comprehensive reporting may lead to either a lower default rate or more availability of credit with the same default rate (but not both). MasterCard stated that, while the actual levels of default and credit availability modelled cannot be achieved simultaneously (given the research assumes holding one parameter constant when modelling the impact of change to the other measure), lower

---

72 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 274.

73 Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 1.

74 See J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 1 August 2007.

75 Consumers' Federation of Australia, *Full-File Credit Report: Is it Really the Answer to Credit Overcommitment?* (2005) <www.consumersfederation.com/documents/PositionPaperFeb05.doc> at 1 August 2007, 2. A similar point is made in Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

76 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

77 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

default rates and greater availability of credit 'are not mutually exclusive' outcomes. Rather, 'the Australian credit marketplace will find a natural balance'.[78]

51.63 In submissions, consumer groups expressed continued concern about the actual impact on the credit market of more comprehensive reporting—particularly in the absence of a 'specific legislative requirement upon all credit providers to lend responsibly having regard to all reasonably accessible data'.[79] The Consumer Credit Legal Centre (NSW) (CCLC) noted that:

> - while credit providers could refuse to extend credit to borrowers who are already over-extended, they could equally target those same borrowers with expensive priced for risk products;
> - while credit providers could use the additional information available to reduce defaults, they could equally use the information to increase lending volumes while maintaining default rates resulting in a larger total number of defaulters;
> - while credit providers could use the additional information to improve the quality of their lending decisions, they could equally use the information to further abridge the application process (by relying on the credit report rather than application data, for example) to compete more effectively on the basis of approval time and price.[80]

51.64 Veda Advantage also noted concerns that more comprehensive reporting might have the effect of pushing marginal consumers out of the formal credit system and into the hands of pay day lenders.[81]

51.65 Some credit providers concede that the overall level of indebtedness is likely to rise, even though the overall proportion of bad loans declines.[82] Westpac, which does not support more comprehensive credit reporting, submitted that 'there is no statistical evidence which establishes the relationship between comprehensive credit reporting and a reduction in levels of over-indebtedness'. Rather, it submitted, international experience with comprehensive reporting strongly supports the view that it can 'lead to increases in personal unsecured lending levels'. In this context, Westpac noted that the level of Australian consumer credit default is low when compared with, for example, the United Kingdom.[83]

---

78 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

79 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 133. The CCLC recommended that stand-alone responsible lending provisions should be introduced into the *Consumer Credit Code*, requiring credit providers to take reasonable steps to ensure that an applicant can meet his/her obligations under the contract without substantial hardship: Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 58.

80 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

81 Veda Advantage, *Submission PR 272,* 29 March 2007.

82 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

83 Westpac, *Submission PR 256,* 16 March 2007.

51.66 Consumer groups have also expressed concern about possible lending and credit pricing practices that might be facilitated by more comprehensive reporting. The CCLC submitted that, for example, the 'use of credit file information to trigger price variations on existing contracts should be expressly prohibited' and warned that an enhanced ability on the part of credit providers to price risk 'should not be accepted as being necessarily in the public interest'.[84]

51.67 More generally, consumer groups are not confident that more comprehensive reporting would automatically result in more responsible lending decisions. The CCLC stated that current casework experience 'suggests that the improvement in responsible lending predicted by the credit reporting agencies will not occur as a consequence of an extended credit reporting system but would have to be specifically imposed by the legislature'.[85]

Problems with more comprehensive credit reporting

51.68 Those against introducing more comprehensive credit reporting challenge some of the claimed benefits. In addition, it is argued that any benefits from the introduction of comprehensive reporting are likely to be outweighed by concerns about information privacy and security.

Impact on privacy and security of personal data

51.69 In IP 32, the ALRC noted disquiet about the impact of comprehensive credit reporting on individuals' privacy rights.[86] Various government inquiries have expressed concern in this regard.[87] The Victorian Consumer Credit Review noted that a system of more comprehensive credit reporting would have a significant 'potential impact on privacy … particularly in relation to financial matters'.[88]

51.70 The CCLC submitted that more comprehensive credit reporting 'is fraught with privacy and security risks', particularly given that it will likely entail 'a large database of information about millions of people [being] maintained by one or more third parties'. In particular, the CCLC was concerned about the following risks:

> - the errors that occur in the current system will increase in proportion to the amount of data, magnifying the above effects;
>
> - [these] data would be potentially very valuable and the temptation to sell it for marketing and other unauthorised purpose could be difficult to resist (if only by unscrupulous employees);

84 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.
85 Ibid.
86 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [6.46]–[6.47].
87 See, eg, Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.46].
88 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 273.

> - this concentration of electronically stored data could also be the target of identity fraudsters and other people with illegal intent.[89]

51.71 Stakeholders elaborated on privacy concerns about more comprehensive reporting. Veda Advantage characterised the privacy risks as involving: first, the risk to the individuals arising from a more significant quantity of data about them being held and shared among credit providers; and secondly, the potential harms arising from the misuse of the data, for both credit and non-credit related purposes.[90]

51.72 Concerns were expressed about the possible use and disclosure of credit information for non-credit related purposes.[91] For example, Westpac stated:

> The introduction of comprehensive reporting also brings with it a significant risk that highly sensitive customer information may be used inappropriately, as the existence of such comprehensive, centralised databases may be mined for data by credit providers and other reporting agencies for marketing purposes.[92]

51.73 Veda Advantage also noted that, with more personal information collected and stored, there may be pressure for secondary use of the data, for example, for employment screening. However, this 'function creep' is 'not in itself a harm for data subjects, but does present challenges for maintaining a tight regime of consumer data protection'.[93]

51.74 The accuracy of the information collected under a more comprehensive credit reporting system was another focus of concern in submissions.[94] For example, the Office of the Privacy Commissioner (OPC) noted that complaints about accuracy 'are often the result of inadequate steps being taken by credit providers to ensure accuracy of information, rather than the volume of information that is available'. On this basis, the OPC said

> it is reasonable to extrapolate that expanding the volume and depth of information that would be available on individuals' credit information files may worsen the current problems with accuracy of credit information.[95]

51.75 The OPC submitted that current problems with inaccuracy 'cannot necessarily be resolved solely by permitting comprehensive credit reporting' and that any proposal

---

89 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

90 Veda proposes to undertake a privacy impact assessment process 'to gain some insights into the risk and mitigants available in a comprehensive environment': Veda Advantage, *Submission PR 272,* 29 March 2007.

91 Issues concerning regulating the use and disclosure of credit reporting information, including any personal information additional to that currently permitted, are discussed in more detail in Ch 53.

92 Westpac, *Submission PR 256,* 16 March 2007.

93 Veda Advantage, *Submission PR 272,* 29 March 2007.

94 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Westpac, *Submission PR 256,* 16 March 2007.

95 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

to introduce more comprehensive credit reporting should be supported by 'standards that would promote a higher level of data accuracy'.[96] Westpac endorsed the view that 'comprehensive reporting would magnify, not minimise, problems associated with the accuracy and integrity of the current credit reporting system'.[97]

51.76 In contrast, credit reporting agencies and some credit providers believed that more comprehensive credit reporting should result in improved accuracy of data.[98] These improvements will result from more frequent and automated reporting[99] (depending on the model of reporting implemented) and more consumer engagement with credit information files.[100] MasterCard stated:

> Overseas evidence suggests that inaccuracies are 'washed out' by the more regular update of an individual's record. Indeed we understand that the vast bulk of credit record errors relate to the consumer's name (such as spelling) and address. With the implementation of more sophisticated screening software (as will be required to support more comprehensive credit reporting) … such errors will be drastically reduced.[101]

51.77 Further, the chances of inaccuracies affecting decisions about granting credit may be reduced because of the presence of other data.[102] For example, the impact of one late payment on an individual's credit score may be mitigated by the balance of that individual's overall repayment history.

51.78 Data security was also cited as a privacy concern. Westpac referred to incidents overseas where the security of comprehensive credit reporting information has been compromised by credit reporting agencies.[103]

51.79 Finally, there was concern about the appropriateness of credit reporting agencies collecting and reporting payment performance information in relation to utilities, such as telecommunications, energy and water.[104] The Telecommunications Industry Ombudsman noted that there 'are numerous reasons why a customer may not be able to

---

96 Ibid.

97 Westpac, *Submission PR 256,* 16 March 2007.

98 ANZ, *Submission PR 291,* 10 May 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

99 Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

100 Veda Advantage, *Submission PR 272,* 29 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007. Under some models of more comprehensive reporting, what is reported to the credit reporting agency will be reflected on the individual's statement of account, greatly reducing the incidence of incorrect default listings: GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

101 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

102 Veda Advantage, *Submission PR 272,* 29 March 2007.

103 Westpac, *Submission PR 256,* 16 March 2007.

104 Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

able to pay their bill on time, many of which do not equate to the customer being a potential credit risk'.[105]

51.80 Submissions from those in favour of more comprehensive credit reporting indicated that the proponents are well aware of these and other privacy concerns. American Express stated, rather than being insurmountable, privacy concerns can be addressed through 'the imposition of legislative controls or general prohibitions on the use of information', strengthened enforcement and more flexible penalties.[106]

51.81 Proponents agree that, if a more comprehensive credit reporting system is to be implemented, there needs to be a range of improvements to the present regulatory regime. These improvements, many of which are desirable whether or not there is a move toward more comprehensive reporting, are discussed in detail in Chapters 52–55.

Empirical studies

51.82 Proponents claim that empirical studies provide important evidence about the likely economic benefits of more comprehensive credit reporting. A number of studies have been referred to in consultations and submissions. These and other relevant studies, including forthcoming research commissioned by Veda Advantage, are discussed briefly below.

51.83 The research most commonly cited in this context is the Barron and Staten research.[107] The results of this research were published in 2000.[108] Barron and Staten compared the position of credit providers in relation to risk assessment under the rules provided by the FCRA in the United States and the *Privacy Act* respectively, using United States data provided by Experian Information Solutions Inc, a leading United States credit reporter. The research compared the accuracy of risk scoring models using the credit reporting variables available under the United States system with the more limited set of variables available in Australia.

51.84 The research found that the more comprehensive form of credit reporting would enable credit providers to achieve a lower rate of defaults on loans, while maintaining the same loan approval rate (for example, at an approval rate of 60%, the Australian variables produced a default rate of 3.35%, as compared to 1.9% for the United States variables). At the same time, assuming that default rates were maintained at the same

---

105 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007. For example, customers may have received an unexpectedly high bill due to inadequate management of utilities provision.

106 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

107 The Barron and Staten research was referred in: Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

108 J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 1 August 2007.

rate (for example, 4%) credit providers using the Australian variables would extend new credit to 11,000 fewer consumers for every 100,000 applicants than would be the case if they were allowed to use the more comprehensive data available under United States law.[109]

51.85 Later research by Barron and Staten, conducted at the request of the Australian Finance Conference (AFC), compared the effect of the United States variables with an 'intermediate model' of credit reporting that allows for the reporting of the 'existence (and type) of accounts that are in good standing or have been paid in full, but does not report current balances or revolving account credit limits'.[110] This 2007 research found that, at the targeted approval rate of 60%, the intermediate model produced a 2.46% default rate.[111]

51.86 The implications of the Barron and Staten research are said to include that consumer credit will be less available and more expensive in countries (for example, Australia) where credit reporting omits categories of variables that would provide a more complete picture of a consumer's financial position.[112]

51.87 Other evidence about the benefits of more comprehensive reporting is said to derive from studies that compare credit reporting regimes in different jurisdictions with the characteristics of the credit markets in those jurisdictions. For example, Tullio Jappelli and Marco Pagano analysed the credit reporting regimes and credit markets in 43 countries, including the US, Australia and most other OECD countries. Their econometric analysis found that the breadth and depth of a credit market was positively associated with the extent of the credit information that is exchanged between lenders.[113]

51.88 In 2003, a United States Congressional Research Service report surveyed the literature (including that already discussed) and concluded that empirical research suggested that privacy laws that restrict the reporting of consumer credit data could lead to the potential loss of significant economic benefits. That is, credit data limitations may increase the cost of consumer credit, reduce accessibility and lower the overall volume of lending.[114]

---

109 Ibid, 20. The more comprehensive credit reporting model would approve 83% of applicants compared to 74% of applicants using the more restricted information.

110 M Staten and J Barron, *Positive Credit Report Data Improves Loan Decision-Making* (2007) Australian Finance Conference.

111 Ibid.

112 J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 1 August 2007, 28.

113 T Jappelli and M Pagano, *Information Sharing, Lending and Defaults: Cross-Country Evidence* (2000) Centre for Studies in Economics and Finance, University of Salerno. The Jappelli and Pagano research was referred to in: MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

114 L Nott, *The Role of Information in Lending: The Cost of Privacy Restrictions* (2003), 9.

51.89 Submissions to this Inquiry have referred to the experience in a range of other countries as support for the view that the introduction of more comprehensive reporting would have significant economic benefits.

51.90 Dun and Bradstreet referred to data from Japan, Hong Kong and Latin America (in addition to placing reliance on the Barron and Staten research). For example, it was said that Hong Kong experienced a dramatic decline in loan defaults following the introduction of more comprehensive reporting in 2002.[115] MasterCard and American Express also referred to the Hong Kong experience.[116] An important qualification to the conclusions drawn is that Hong Kong's economy began to recover from a recession in this period, and it is possible that this recovery was a more important cause of the decline in loan defaults than credit reporting reform.

51.91 Other studies cast doubt on the relationship between more comprehensive credit reporting and credit market efficiency. Jentzsch and San José Riestra created a 'credit reporting regulatory index' for 27 jurisdictions in Europe and the United States, which measured the extent of information privacy regulation affecting credit reporting. Their research found that while increased coverage of credit reporting (in terms of the number of credit reports issued scaled by population) is associated with increasing access to credit, there is no evidence that privacy restrictions greatly hamper information sharing in consumer credit markets.[117]

51.92 Finally, research has modeled the macro-economic impact of introducing more comprehensive credit reporting in Australia.[118] The MasterCard/ACIL Tasman report concluded that comprehensive credit reporting would generate a one-off increase in capital productivity of 0.1 per cent, which would translate to economic benefits to the Australian economy of up to $5.3 billion, in net present terms, over the next ten years.[119]

---

115 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

116 MasterCard Worldwide claimed that, in Hong Kong, material defaults by individuals fell by 27% following the introduction of comprehensive credit reporting: American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007. See also Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 17.

117 N Jentzsch and A San José Riestra, 'Consumer Credit Markets in the United States and Europe' in G Bertola, R Disney and C Grant (eds), *The Economics of Consumer Credit* (2006) 27, 51.

118 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004). The ACIL Tasman research was referred to in: MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

119 ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3. See also ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 28.

51.93 ACIL Tasman used what was described as an 'applied general equilibrium model' of the Australian and world economies to quantify the benefits of more comprehensive credit reporting. The model assumed that 'the efficiency of the credit market has implications for the efficiency of virtually every sector of the economy',[120] and took as one starting point the Barron and Staten findings about the possible reduction in the rate of default if a US-style comprehensive reporting system was adopted.[121]

The limitations of empirical studies

51.94 There is debate about the conclusions it is appropriate to draw from empirical studies of the effects of more comprehensive credit reporting on credit markets and the economy, especially in view of methodological limitations and the assumptions built into research models. On one view, the subject matter does not lend itself to precise modelling due to the level of complexity and the small orders of magnitude involved in terms of benefits. It is questionable, therefore, that any modelling will provide definitive answers.

51.95 For example, it may be observed that the Barron and Staten research—in comparing the accuracy of credit scoring using variables available under the United States system with the more limited set of variables available in Australia—disregarded the 'positive' information provided on application forms.

> Their results are not directly comparable to actual experience in the Australian market, because they do not factor in the additional (though limited) predictive value of the additional demographic data that Australian lenders generally use to make up that difference.[122]

51.96 The Victorian Credit Review noted that, in order to consider fully the possible benefits of more comprehensive reporting in assessing capacity to repay, research would need to show a material gap between the information provided by the consumer and in a more comprehensive credit report. That is, whether the information sourced directly from consumers

> is materially less helpful to assessing capacity to repay than that from a positive credit reporting agency having regard for:
>
> - weight given to negative information rather than positive information generally;
> - existing capacity to verify positive information, albeit through a more costly process of having to contact other credit providers individually;
> - likely inaccuracies in the data;

120 ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 3.

121 Ibid, 24.

122 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

- the potential use of profit scoring[123] mechanisms;
- other factors independent of this information that may be more material to repayment capacity, such as loss of job, death/separation from spouse, etcetera.[124]

51.97 Further, different macro-economic environments limit the applicability of conclusions drawn from international experience about the possible effects of more comprehensive reporting on levels of default, credit availability and interest rates in Australia. There are many factors, relating to credit markets and macro-economic conditions generally, which have an influence on these outcomes.

51.98 For example, Australia is recognised as having a credit market that is very competitive by international standards. This may limit the potential for competitive gains resulting from more comprehensive reporting. Equally, a macro-economic upturn seems likely to have a much greater influence on credit availability than any change to a credit reporting system.

Veda Advantage research

51.99 Some of the limitations in available evidence about the likely impact of more comprehensive reporting may be addressed by new research proposed by Veda Advantage. Veda Advantage has advised that it is working on research proposals to:

- study the potential effects on lending behaviour and consumers, of more comprehensive credit reporting, using Australian data (the data study); and
- model the micro-economic and allocative effects of more comprehensive credit reporting in Australian credit markets, and the impact on different cohorts of consumers (the economic study).[125]

51.100 The data study is intended to model the effect that comprehensive consumer credit reporting will have on the accuracy of credit providers' application risk evaluation. Veda Advantage proposes to use information from its existing credit reporting database and more comprehensive 'positive' information, including credit card application, account and payment histories, provided by participating credit providers.[126]

---

123 'Profit scoring' essentially refers to a score that takes into account profits generated from late payments, for example, rather than the actual risk. Accordingly, risk reduction may compete with profit scoring: Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 261.

124 Ibid, 260. In April 2005, ANZ conducted a trial of completed statements of financial position provided by customers applying for a credit limit increase in the ACT. The study found that 24% of forms had errors and omissions in financial details: ANZ, *Submission PR 291,* 10 May 2007.

125 Veda Advantage, *Submission PR 272,* 29 March 2007.

126 Ibid.

51.101 The economic study is intended to draw correlations between financial markets that have different forms of credit reporting regulation in order to model how Australian financial institutions are likely to change their lending practices in response to more comprehensive credit reporting. The primary source of data for this study will be international literature on comprehensive reporting and lending practices, supplemented by the results of the data study, micro-economic modelling, statistics provided by overseas credit providers and credit reporting agencies, and interviews with financial institutions.[127]

Regulation in other jurisdictions

51.102 As discussed above, the credit reporting provisions of Part IIIA provide an exhaustive list of the kinds of personal information that may be included in a credit information file or credit report. The collection of other kinds of information, including information about credit granted to individuals—such as credit limits or current balances—is not permitted. The following material considers how this aspect of credit reporting is regulated in other jurisdictions.[128]

New Zealand

51.103 New Zealand is another jurisdiction in which more comprehensive credit reporting is effectively prohibited. In that jurisdiction, credit reporting is regulated by a binding code issued by the Privacy Commissioner under the *Privacy Act 1993* (NZ).[129]

51.104 The *Credit Reporting Privacy Code 2004* (NZ) (the NZ Code) provides that a credit reporting agency must not collect personal information for the purpose of credit reporting unless it is 'credit information'.[130] Briefly, credit information is defined exhaustively and includes identification information, information about credit applications, credit default information, judgment and bankruptcy information, serious credit infringements and information from public registers.[131]

51.105 While the information permitted by the NZ Code is in some respects broader than that permitted under Part IIIA,[132] the permitted content of credit reports closely replicates the position in Australia. Importantly, the NZ Code does not permit a credit reporter to collect information about an individual's current credit commitments and facilities.

---

127 Ibid.

128 Material on the regulation of credit reporting in other jurisdictions is drawn, in part, from: Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006).

129 *Credit Reporting Privacy Code 2004* (NZ) under *Privacy Act 1993* (NZ) s 46.

130 *Credit Reporting Privacy Code 2004* (NZ) r 1(2).

131 Ibid cl 5.

132 For example, the New Zealand Code allows the collection of 'information relating to identification documents reported lost or stolen or otherwise compromised' and 'credit scores': Ibid cl 5.

United States

51.106 In the United States, credit reporting is regulated under the *Fair Credit Reporting Act 1970* (US) (FCRA) by the Federal Trade Commission. The FCRA does not limit the permissible content of credit information files held by credit reporting agencies or the content of credit reports—although, for example, consumers must consent in writing to the disclosure of reports containing medical information.[133]

51.107 Major credit reporting agencies in the United States hold and report detailed information about individuals' credit accounts including, but not limited to, current balances, credit limits, amounts past due, payment performance and payment status pattern and account descriptions.[134]

51.108 Credit reporting agencies receive information from credit providers and others, generally every month, and update their credit files within one to seven days of receiving new information.[135]

United Kingdom

51.109 In the United Kingdom, credit reporting agencies are regulated by both the *Consumer Credit Act 1974* (UK) and the *Data Protection Act 1998* (UK)—the latter being the equivalent in the UK of the Australian *Privacy Act*.

51.110 Neither the *Consumer Credit Act* nor the *Data Protection Act* specifically limits the permissible content of credit information files. The *Consumer Credit Act* deals only with individuals' rights of access to, and correction of, credit information about them.[136] Under the *Data Protection Act*, a 'data controller' (which may include a credit reporting agency) must comply with the data protection principles (DPPs) set out in the Act. These include DPP 3, which provides that 'personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'.[137]

51.111 The information held by credit reporting agencies in the United Kingdom, and included in credit reports, includes: data about the date accounts are opened; the credit limit or amount of the loan; payment terms; payment history; and payment arrangements entered with the credit provider.[138] Unlike in the United States, information on credit account balances is not collected.

---

133 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US).

134 R Avery and others, 'An Overview of Consumer Data and Credit Reporting' (2003) (February) *Federal Reserve Bulletin* 47, 54.

135 Ibid, 49.

136 *Consumer Credit Act 1974* (UK) ss 157–160.

137 *Data Protection Act 1998* (UK) sch 1, pt 1.

138 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 79; United

Other jurisdictions

51.112 A 2006 report prepared for MasterCard Worldwide (the MasterCard/CIE/EDC Report) summarised the key features of the regulatory systems for credit reporting in more than a dozen countries.[139] All the countries studied, with the exception of France, were said to permit more comprehensive credit reporting than in Australia.

51.113 A comparison was made of the kinds of information held by credit reporting agencies in Australia, the United States, the United Kingdom, Germany, Canada, Japan, Hong Kong and Singapore.[140] This showed that in all countries except Australia, credit reporting agencies collect information about individuals' credit limits and payment history. In addition, credit reporting agencies in the United States, Japan and Hong Kong also hold information about individuals' credit account balances.

51.114 In the last few years, some jurisdictions have moved from reporting only negative information, such as overdue payments, to more comprehensive credit reporting. For example, in 2003, Hong Kong implemented a regime of more comprehensive credit reporting, in part due to concern about levels of debt default and bankruptcy.[141] The Hong Kong Monetary Authority considered that the sharing by banks of more comprehensive information—through credit reporting agencies and subject to information privacy legislation—would help to promote a more effective banking system.[142]

Lessons for Australia

51.115 Stakeholders that advocated more comprehensive credit reporting continued to contrast the position in Australia with that in jurisdictions overseas. For example, Veda Advantage noted that, in the past five years Hong Kong, Belgium, Greece, India and South Africa have all implemented models of more comprehensive reporting.[143] American Express highlighted the advantages of the systems in the United States, United Kingdom, Hong Kong and Canada.[144]

Kingdom Government Information Commissioner's Office, *Data Protection: Credit Explained* (2006), 8, 13.

139 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006). The countries reviewed include the United States, Canada, the United Kingdom, Germany, France, Italy, Belgium, South Africa, Japan, Hong Kong, South Korea, Singapore, Mexico and selected countries in central and South America.

140 In some of these jurisdictions, credit reporting information is held by public credit registries rather than private sector credit reporting agencies. Public credit registries are operated by governments, usually banking and finance industry regulators that are similar, for example, to the Australian Prudential Regulation Authority: see Ibid, 9–11.

141 Ibid, 112.

142 Ibid, 112.

143 Veda Advantage, *Submission PR 272,* 29 March 2007.

144 American Express, *Submission PR 257,* 16 March 2007.

51.116 While most other comparable jurisdictions permit credit reporting agencies to collect a broader spectrum of information than is permitted in Australia, this is not universally true. A number of jurisdictions—such as France, Spain and New Zealand—possess comparable restrictions to Australia in relation to the types of personal information that may be collected and used in credit reporting.[145]

Models of more comprehensive credit reporting

51.117 In IP 32, the ALRC noted that lack of consensus regarding a preferred model of comprehensive reporting has hindered debate about whether more comprehensive reporting should be introduced, including in the context of previous government inquiries.[146]

51.118 The following part of this chapter examines the spectrum of views about the categories of personal information that should be able to be collected as part of a more comprehensive credit reporting system. The chapter also considers, more briefly, other related aspects of regulation seen by stakeholders as necessary in a move to allow more comprehensive reporting. The Discussion Paper returns to some of these issues in Chapters 52–55.

New categories of personal information

51.119 In IP 32, the ALRC asked whether Australian law should be amended to expand the categories of personal information that may be collected and used in credit reporting and, if so, what categories of personal information should be permitted.[147] A range of responses were received, from those suggesting loosening prohibitions on the content of credit reporting information through to those suggesting only minor extensions in the content currently permitted under s 18E of the *Privacy Act*.

51.120 The following discussion focuses only on categories of personal information that concern an individual's current credit commitments or repayment performance. Chapter 52 deals with the collection of other categories of personal information, such as identifying information.

---

145 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 12; J Peace, 'Knowing Your Customer: An Advantage for Business and Individuals?' (Paper presented at 28th International Conference of Data Protection Commissioners, London, 2 November 2006).

146 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [6.72] citing, eg, Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 273. In its response to the Victorian Consumer Credit Review, the Victorian Government observed that this lack of consensus makes it difficult to determine whether more comprehensive credit reporting would in practice 'enhance decision making' by credit providers: Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 46.

147 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 6–3.

51.121 The Australasian Retail Credit Association (ARCA) submitted that the *Privacy Act* should be amended to 'remove the barrier to comprehensive reporting and focus on defining what is not allowed rather than having proscriptive legislation'.[148] Broadly, ARCA favours an approach similar to that in the United Kingdom where legislation does not specifically limit the permissible content of credit reporting information files.[149]

51.122 In the United Kingdom, under the *Data Protection Act*, a credit reporting agency must only comply with DPP 3, which provides that 'personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'. In Australia, the equivalent would involve leaving the potential content of credit information files to be restricted only by National Privacy Principle (NPP) 1.1, which provides that an organisation 'must not collect personal information unless the information is necessary for one or more of its functions or activities'.

51.123 ARCA does not hold a firm view on the precise data items that should be collected as part of more comprehensive credit reporting. An important aspect of its position is that the credit reporting system needs to be flexible, in order to respond to the changing needs of credit providers and individuals. Similarly, the AFC stated that ALRC should not

> make the 1989 mistake of specifying (and freezing in time) credit report permitted content but should recommend that such content be developed by the Privacy Commissioner in consultation with industry, community groups and government agencies … so that statistical, systems and public aspirational issues, in addition to legal ones, can be taken into account and evolve over time.[150]

51.124 GE Money submitted that credit reporting agencies should be permitted to collect and use

> a comprehensive range of data (with mandated minimum content) for evaluating credit risk and capacity to repay, collections purposes (specifically, 'clear out') and for anti-money laundering and fraud prevention.[151]

51.125 In relation to payment performance data, GE Money recommended that to 'ensure optimal credit risk assessment capability' the following data should be collected by credit reporting agencies:

- product eg, credit card, personal loan;
- start date;
- closed date;

---

148 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007. St George Bank supported the ARCA submission: St George Banking Limited, *Submission PR 271,* 29 March 2007. Veda Advantage expressed a similar view, stating that 'legal framework should seek to proscribe information that is not permitted rather than prescribing in detail what is': Veda Advantage, *Submission PR 272,* 29 March 2007.

149 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

150 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

151 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

- initial advance or credit limit;
- current balance;
- 24 months repayment history and current payment status;
- date of last payment;
- account status eg. written off, inactive etc;
- date of account status;
- monthly repayments;
- worst ever delinquency status;
- amount of write-off;
- current unpaid write-off;
- date debt sold (if sold to a third party);
- value of debt at time of sale (if sold to a third party) ...[152]

51.126 Other credit providers also favoured the collection of an extensive range of information about accounts, repayment performance and current credit commitments. American Express referred to the need to collect repayment performance and current credit commitment data on a monthly basis, which 'at the very least contains the total limits on credit facilities or available credit and the individual's total liabilities'.[153] MasterCard supported recommendations made in the MasterCard/CIE/EDC Report.[154] These recommended that information about an individual's repayment performance and current credit commitments include the following:

> Institution; type of credit; term of credit (eg, fixed, open ended); security (secured, unsecured); account open date; account ownership (individual, joint, guarantor, Director, etc); amount of credit granted (refreshed if changed); current month balance; current month past due amount (if applicable); 24 month repayment performance history (categories: current, 1–29, 30–59, … 150–179, 180+); account close date.[155]

51.127 Veda Advantage favoured the collection of 'the widest range of data necessary to inform credit markets', and suggested the collection of categories of repayment and credit commitment information similar to those favoured by GE Money.[156]

---

152 Ibid. GE Money also recommended that collection of 'extended credit application summary' data for anti-money laundering and fraud prevention: see Ch 53.

153 American Express, *Submission PR 257,* 16 March 2007.

154 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006).

155 Ibid, 51.

156 Veda Advantage, *Submission PR 272,* 29 March 2007. The categories were: credit facility type; account status; date opened; date closed; days past due; credit limit; outstanding credit balance; highest credit balance; term of credit; collateral type, value and date of valuation; scheduled payment amount; actual payment amount; amount past due; date of last payment; last activity date; reason for closure; amount of write-off.

51.128 Another credit reporting agency, Dun and Bradstreet, has proposed a model of more comprehensive credit reporting, which is said to avoid some of the features of the more permissive regime of credit reporting in the United States and to be 'a modified, fairer version that provides more limited but valuable data'.[157] Dun and Bradstreet recommended that the *Privacy Act* be amended to permit credit reports to contain 'four additional data elements':[158]

- type of account—eg, personal loan, credit card;
- credit provider;
- credit limit;
- date account is opened.[159]

51.129 Some credit providers considered that these categories of information are the minimum necessary to deliver benefits in credit decision making. On the other hand, this more limited model of more comprehensive reporting has been criticised by others in the credit industry. For example, GE Money states that the Dun and Bradstreet model is inadequate because, among other things, it 'lacks the most predictive risk data that is the repayment history'.[160] GE Money also expressed concerns about competitive neutrality in that a limited model of more comprehensive reporting

> may be acceptable in connection with products that have a long application 'life-cycle' (mortgages for example), but could not be operationalised in relation to 'on the spot' products such as store credit applications. Any such limited model would confer a competitive disadvantage on providers of short application life-cycle products.[161]

51.130 In its submission, the OPC noted that the *Privacy Act* already allows a credit report to contain a record of a prospective credit provider having sought a credit report on an individual in relation to a credit application and the amount of the application;[162] and allows the credit provider to list themselves as being a current credit provider when the credit is advanced.[163] The OPC submitted that:

> In addition to these two categories of information, the Office believes consideration should be given to including provisions which allow: a credit provider to note on an individual's credit information file on a voluntary basis that an offer of credit was accepted without specifying the actual amount ...[164]

Reciprocity and reporting

51.131 In IP 32, the ALRC asked, if Australian law is amended to permit more comprehensive credit reporting, what changes should be made to the way in which

---

157 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 11,* 13 April 2006, Annexure (Briefing Note), 5.
158 *Privacy Act 1988* (Cth) s 18E(1)(b)(v) already allows a credit provider to list themselves as being a current credit provider on an individual's credit file.
159 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.
160 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.
161 Ibid.
162 *Privacy Act 1988* (Cth) s 18E(1)(b)(i).
163 Ibid s 18E(1)(b)(v).
164 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

personal information is collected and disseminated for the purposes of credit reporting. For example, the ALRC asked whether it would be desirable to make personal credit information available to a broader or narrower spectrum of individuals and organisations than may currently access such information; and whether there should be differential levels of access to personal information that is collected under such a system.[165]

51.132 There was considerable support in submissions for the principle of reciprocity in credit reporting.[166] In relation to data sharing among credit providers, this principle has been expressed as dictating that 'data will be shared on the principle that subscribers receive the same credit performance level data that they contribute, and should contribute all such data available'.[167]

51.133 All credit providers interviewed in the course of research by the CCLC were reported as being 'convinced of the benefits of reciprocity in ensuring the completeness of credit reporting data'.[168] One of the main aims of ARCA, a peak body of credit providers interested in the operation and reform of the credit reporting system, is to improve data standards and consistency, including by promoting the principle of reciprocity.[169]

51.134 GE Money submitted that principles of reciprocity should be legislatively mandated as part of a system of more comprehensive credit reporting. GE Money also considered that 'in order to ensure the ongoing commitment to a comprehensive credit reporting model from credit providers with large market share', participation should be mandatory.[170] Abacus stated that access to more comprehensive credit reporting should be

> based on mandatory information collection to ensure users have a stake in the quality and safety of data collected–although caution should be exercised not to lock out smaller credit providers …[171]

51.135 In contrast, American Express submitted that more comprehensive reporting should be introduced on a voluntary basis, but that voluntary participation should not

---

165 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 6–4.

166 Confidential, *Submission PR 297,* 1 June 2007; ANZ, *Submission PR 291,* 10 May 2007; Optus, *Submission PR 258,* 16 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

167 Steering Committee on Reciprocity, *Information Sharing: Principles of Reciprocity* (2003), 3.

168 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 60.

169 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

170 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007. See also Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

171 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

continue indefinitely as the efficiency and utility of the system can only be maximised through the participation of all credit providers. Telecommunications companies AAPT and Optus also stated that contributing data to a more comprehensive credit reporting system should not be mandatory.[172]

51.136 Reciprocity is one means by which access to enhanced credit reporting information could be differentiated—so that, for example, some subscribers may obtain information about debt default, but not other information about current credit commitments and repayment performance. It has been suggested that telecommunications companies should continue to contribute only 'negative' default and other credit information and, in turn, they should be entitled to receive reports based only on those categories of information.

51.137 Some submissions referred to the desirability of 'tiered' access, including in relation to non-credit related purposes, such as debt collection and identity verification.[173] Tiered access can be based on reciprocity, or take other factors into account so that subscribers may obtain some categories of information that they do not provide to the agency. For example, some companies might be permitted to use credit reporting information for identity verification, despite not providing information on their own customers. Veda Advantage supported tiered (full or summary only) access to credit reporting information based on:

- reciprocity;
- data protection compliance standards;
- use context;
- harm prevention;
- participation in an ASIC approved EDR scheme.[174]

Type of credit reporting agency

51.138 In IP 32, the ALRC discussed whether, if Australian law is amended to permit more comprehensive credit reporting, there should be any consequential changes to the way in which personal information is collected, and what kind of bodies should be permitted to act as a credit reporting agency.[175]

51.139 Currently, personal information may be collected for credit reporting purposes by credit reporting agencies, and agencies charge credit providers a fee in return for disclosing some of that information in a credit report. Those consumer credit reporting agencies currently operating in Australia are private enterprises that carry out

---

172 AAPT Ltd, *Submission PR 260,* 20 March 2007; Optus, *Submission PR 258,* 16 March 2007.

173 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007.

174 Veda Advantage, *Submission PR 272,* 29 March 2007.

175 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [6.77]–[6.79].

a business for profit. The CRAA, previously the dominant Australian consumer credit reporting agency, however, was a not-for-profit association established by the finance industry.

51.140 Some overseas models, like the United States and United Kingdom, adopt a similar approach to Australia's, by allowing private enterprises to act as credit reporting agencies. Some other jurisdictions permit more comprehensive credit reporting but have a different form of credit reporting agency. Alternative models include industry-owned credit reporting agencies that operate on a not-for-profit basis; and government-operated credit information databases (also known as public credit registries).[176]

51.141 The CCLC submitted that, in Australia, any credit reporting agency should be a non-profit, licensed or state owned, monopoly. It was suggested that this would:

- improve public confidence in privacy protection;
- ensure easy consumer access to reports and information (no multiple credit reporting agencies);
- improve transparency;
- expedite reform processes by removing the vested interests of credit reporting agencies from any debate (balancing the needs of credit providers with the needs of consumers only); and
- remove conflict of interest between the commercial imperative and the public interest.[177]

51.142 Otherwise, submissions and consultations did not indicate any support for regulatory change in this regard. MasterCard observed that any move towards a single 'centrally maintained database to hold credit information' would 'prevent the obvious benefits that would arise from a competitive credit reporting industry, including technology enhancements, competition in data quality and pricing'.[178] The ALRC observes, however, that the arguments for placing credit reporting databases under government or public control become stronger as the information held on them becomes more comprehensive.

---

176 See, Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006).

177 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 42.

178 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

Privacy safeguards

51.143 In IP 32, the ALRC asked, if Australian law is amended to permit more comprehensive credit reporting, whether any additional safeguards should be introduced to protect the privacy of personal information.[179]

51.144 The CCLC submitted that if the implementation of a more comprehensive credit reporting system is to be considered:

- The purpose of the credit reporting system should be clearly defined;
- The type of data able to be collected and the level of access to that data should be limited to only what is the most relevant or necessary to achieving that purpose;
- There should be adequate rights for consumers in relation to accessing their report, understanding their report and how it is used;
- There should be robust and rigorous dispute resolution schemes in place;
- There should be adequate safeguards to ensure the security and integrity of the data;
- There should be a specific legislative requirement on lenders to lend responsibly having regard to all readily available information; and
- There should be safeguards to ensure that the system is not used to exacerbate or entrench financial hardship, such as prohibitions on access by employers or real estate agents, for marketing or for triggering price differentials on existing accounts.[180]

51.145 The Australian Privacy Foundation considered that individuals should be given a choice about whether more comprehensive credit reporting information should be provided to agencies. The Foundation stated that this should be on a consent or opt-in basis, 'rather than either an implied consent or "opt-out" basis, or simply being notified that it was a condition of a loan application'.[181]

51.146 Submissions from credit providers and credit reporting agencies also highlighted the need to consider the adequacy of existing privacy protections. Veda Advantage submitted that consideration should be given to allowing individuals to opt-in or opt-out of providing 'positive' information.[182] Credit providers and credit reporting agencies also referred to the need for strict prohibitions on the use of credit

179 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 6–4.
180 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.
181 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.
182 Veda Advantage, *Submission PR 272,* 29 March 2007.

reporting information in marketing,[183] improved complaint and dispute resolution mechanisms,[184] and data governance standards.[185]

Should more comprehensive reporting be permitted?

51.147 Submissions to the ALRC Inquiry indicated broad support for the implementation of more comprehensive reporting among credit providers and other subscribers to the existing credit reporting system.[186] Consumer groups, privacy advocates and regulators generally opposed more comprehensive credit reporting.[187] The benefits of, and problems associated with, more comprehensive reporting as perceived by these stakeholders are discussed throughout this chapter.

51.148 Many of those who opposed the introduction of more comprehensive credit reporting submitted that the focus of the present Inquiry should be on reforms to improve the current credit reporting system, before any consideration of its extension.[188] In this context, in IP 32, the ALRC noted earlier suggestions that implementing comprehensive credit reporting is not the only possible, nor necessarily the best, way of improving the current reporting regime.[189] For example, the Victorian Review noted that alternatives to both the status quo and comprehensive credit reporting include:

- Improving the existing negative reporting scheme in terms of its accuracy.

---

183 See, eg, St George Banking Limited, *Submission PR 271,* 29 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

184 See, eg, St George Banking Limited, *Submission PR 271,* 29 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

185 See, eg, Veda Advantage, *Submission PR 272,* 29 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

186 Confidential, *Submission PR 297,* 1 June 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007; Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; St George Banking Limited, *Submission PR 271,* 29 March 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; AAPT Ltd, *Submission PR 260,* 20 March 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007. Support for more comprehensive reporting among credit providers was not universal: Westpac, *Submission PR 256,* 16 March 2007.

187 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Westpac, *Submission PR 256,* 16 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

188 See, eg, Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Westpac, *Submission PR 256,* 16 March 2007.

189 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [6.48]–[6.52].

- Providing additional incentives for credit reporting agencies to maintain accurate and complete data. For example, requiring credit reporting agencies to pay a specified amount to a consumer in each case where information is reported as inaccurate may assist in addressing current information asymmetry within the current system.
- Requiring consumer declarations in relation to loan applications.
- Expanding financial literacy programs to encourage better self-selection by consumers and shopping for credit by consumers.[190]

51.149 In response to IP 32, Westpac submitted that improvements to aspects of the current system were a 'viable and preferable alternative' to the introduction of more comprehensive reporting.[191] Westpac proposed, among other things: introducing compulsory, uniform default reporting requirements; developing a consumer education program; simplifying complaint and dispute resolution processes; addressing issues of inaccuracy in reporting; and introducing a requirement that debtors be advised when a default has been listed.

> In essence, ensuring the data integrity within the current (negative) reporting scheme must be the focus in the short term. The changes suggested above would help to improve the accuracy of the current credit reporting system to the benefit of both consumers and credit providers.
>
> Westpac recommends that these suggestions be implemented and after a reasonable period of time (say 3 years), their effectiveness in addressing the issues identified assessed, before any decision is made to proceed with significant reform of the current credit reporting system.[192]

51.150 Similarly, the Australian Privacy Foundation submitted that the ALRC should recommend that any further consideration of comprehensive reporting be 'deferred until after experience with an initial round of reforms resulting from the current Review'.[193] National Legal Aid also stated that it would oppose the introduction of more comprehensive reporting 'until there is positive progress on addressing the major defects of the current scheme'.[194]

51.151 One particular focus of debate concerning the efficacy of the present credit reporting system involves the reporting of 'current credit provider' status, as permitted under s 18E(1)(b)(v). From one perspective, a record of current credit provider status is 'positive' information, showing that the individual has been granted a credit facility. The ALRC understands that it is not common for credit providers to report that they are current credit providers in respect to individuals. Credit providers do not report current credit provider status because 'the costs outweigh the marginal benefits of providing the information'.[195] In this context, GE Money noted:

---

190 Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 272.
191 Westpac, *Submission PR 256,* 16 March 2007.
192 Ibid.
193 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.
194 National Legal Aid, *Submission PR 265,* 23 March 2007.
195 Veda Advantage, *Submission PR 272,* 29 March 2007.

> The cost of contributing 'full' data files under a comprehensive reporting model would be significantly less than the cost of reporting limited data at 'triggers' such as number or days overdue for payment. This is the reason that GE Money (and other credit providers) does not take advantage of the ability to note that it is a 'current credit provider' on a customer's credit file—the cost of doing so far exceeds the benefit that can be gained from such a limited notation on a consumer credit file.[196]

51.152 The OPC suggested that that if s 18E(1)(b)(v), and other provisions that allow credit providers to share information between themselves with the consent of individuals,[197] were being fully utilised, the introduction of more comprehensive credit reporting may be unnecessary.[198]

51.153 The Banking and Financial Services Ombudsman (BFSO) noted that credit providers can reduce information asymmetry 'by asking for details of all current credit facilities as part of the application process and requiring consumer declarations as to the accuracy of the information'. Therefore, addressing the 'absence of a comprehensive dispute resolution regime and the ability to report unregulated credit … would appear to be the more immediate priorities'.[199]

51.154 A number of submissions suggested that further study is required before reaching any decision to recommend the implementation of more comprehensive credit reporting.[200] The CCLC submitted that:

> Any change to increase, or substantially alter, the permitted categories of data held by credit reporting agencies should be preceded by independent local research with a view to estimating the effect of any proposed change on:
>
> - over-indebtedness;
> - access to affordable credit, including for those who are socially or economically disadvantaged.[201]

---

196 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007. The ALRC observes that, from one perspective, the cost of reporting information always outweighs the benefit to the credit provider who reports it. The benefit comes from access to information reported by *other* credit providers.

197 *Privacy Act 1988* (Cth) ss 8N(1)(b), 18N(1)(be).

198 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007. See also, Queensland Law Society, *Submission PR 286,* 20 April 2007.

199 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007. The Consumer Action Law Centre also considered that improved complaint handling and enforcement mechanisms should be more of a priority than the possible introduction of more comprehensive reporting: Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

200 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

201 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

51.155 ANZ suggested that Treasury should undertake an assessment of the social and economic impact of introducing more comprehensive credit reporting.[202] The OPC also recommended that independent research be conducted on the impact that comprehensive credit reporting would have on the Australian financial system and Australian consumers.[203] The OPC suggested that the research should provide recommendations about:

1. Whether comprehensive credit reporting should be introduced in Australia; and
2. If comprehensive credit reporting were to be introduced:

- what model should be adopted;
- which industry participants should be included in the expanded system; and
- and what compliance framework should be imposed.[204]

ALRC's view

51.156 The ALRC recognises that, according to widely accepted economic theory, making more information available to credit providers will tend to increase efficiency in the market for credit and assist in making credit more available to those able to repay and reduce rates of default (or both).[205] There was no significant disagreement among stakeholders that more comprehensive credit reporting should improve risk assessment by credit providers, even among those who expressed concerns about how this improved risk assessment will be used in the credit market.[206]

51.157 Submissions have highlighted opposing views about the significance of available empirical evidence about the likely effects of more comprehensive credit reporting on the Australian credit market and economy. It has been suggested that answering questions about what information should be collected for the purposes of credit reporting in Australia—or what information is 'necessary' in terms of information privacy principles[207]—requires some form of economic analysis or modelling.[208]

51.158 Suggestions have been made that the ALRC should itself conduct or commission such research. In view of the difficulties and limitations of such studies,

---

202 ANZ, *Submission PR 291,* 10 May 2007. ANZ stated that the 'complexity and importance of this issue would require the appointment of an expert panel, including consumer representatives, to define the operational aspects of the model'.

203 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

204 Ibid.

205 See, eg, the literature reviews in J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance <www.privacyalliance.org/resources/staten.pdf> at 1 August 2007; ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004).

206 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Westpac, *Submission PR 256,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

207 For example, in terms of *Privacy Act 1988* (Cth) sch 3, NPP 1.1.

208 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

and taking into account the Inquiry's timetable and available resources, the ALRC considers that such a course is not practicable.

51.159 The ALRC welcomes further research, including that proposed by Veda Advantage. It notes, however, that there remain significant practical difficulties in conducting such studies—not least because the ideal methodology requires a pre-judgment to be made about the items of personal information that would be available under a more comprehensive credit reporting system. More fundamentally, any credit reporting system is only one tool, albeit an important one, used by lenders to assess risk and to determine lending practices. This tool can be used in different ways, which may depend on other factors including, for example, a particular credit provider's competitive position in the market. The information available through the credit reporting system ultimately cannot dictate what lending practices will emerge or prevail in the marketplace.

51.160 Even assuming that increasing access to credit is necessarily economically beneficial,[209] research results cannot determine the policy position to be adopted. Any proven economic benefit still needs to balanced against individual privacy rights and the risk of breach of those rights. An appropriate balance needs to be struck between efficiency in credit markets and privacy protection.

51.161 There are many possible approaches to reform of the credit reporting provisions to permit more comprehensive credit reporting. The spectrum of choice ranges from recommending no changes in the categories of information now permitted under s 18E of the *Privacy Act* through to recommending that the existing provisions dealing with the permitted content of the credit information files be repealed.

51.162 In the latter case, it would be expected that the provisions of the NPPs—or the 'Collection' principle in the proposed Unified Privacy Principles (UPPs)—would provide some limits on content. The 'Collection' principle would provide that 'an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities'.[210] In addition, the legislative proscription on including certain categories of personal information in credit information files could be retained.[211]

51.163 The ALRC does not favour removing regulation dealing with the permitted content of credit reporting information. Any such move would create uncertainty as to

---

209 The validity of this assumption has been questioned: see, eg Consumer Affairs Victoria, *The Report of the Consumer Credit Review* (2006), 257; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

210 See Ch 18.

211 *Privacy Act 1988* (Cth) s 18E(2) prohibits personal information recording an individual's (a) political, social or religious beliefs or affiliations; or (b) criminal record; or (c) medical history or physical handicaps; or (d) race, ethnic origins or national origins; or (e) sexual preferences or practices; or (f) lifestyle, character or reputation.

the scope of information that may be 'necessary' to assess credit risk or for other functions or activities of credit reporting agencies or credit providers.

51.164 The ALRC's preliminary view is that there should be a modest extension in the categories of personal information that may be collected for credit reporting purposes. Specifically, credit reporting agencies should be able to collect:

- the type of each current credit account opened (for example, mortgage, personal loan, credit card);
- the date on which each current credit account was opened;
- the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and
- the date on which each credit account was closed.[212]

51.165 This extension of the current reporting system has some support from both industry and consumer groups. Importantly, credit providers would have access to more information about an individual's current credit commitments to assist in promoting responsible lending. The proposed extension in credit reporting information would provide much of the additional predictiveness desired by proponents of more comprehensive reporting.[213]

51.166 Under the proposed system, credit providers would be aware of an individual's major potential commitments.[214] The additional categories of credit reporting information would assist to highlight discrepancies with the information provided by the individual credit applicant. The fact that credit providers may be reluctant, for reasons of time and cost, to undertake further inquiries of other credit providers is not a sufficient reason to permit the collection and disclosure of detailed repayment performance and current balance information. As discussed in Chapter 1, an argument for greater access to personal information based on reduced cost to data custodians, or customer convenience, generally will not tilt the balance in favour of reduced privacy protection.

51.167 In order for this reform to benefit the operation of the credit market, reporting by credit providers of the additional data items needs to be as universal as

---

212 These categories of information would replace 'current credit provider' status under Ibid s18E(1)(b)(v).

213 The Barron and Staten (2007) research found that an 'intermediate model' between the existing Australian and United States credit reporting systems would provide 'some 71% of the reduction in delinquencies achievable under the full US scenario': M Staten and J Barron, *Positive Credit Report Data Improves Loan Decision-Making* (2007) Australian Finance Conference, 6. The ALRC's proposed model allows additional categories of credit reporting information to those under the assumed 'intermediate model' and would, therefore, be more rather than less predictive.

214 Further, matching information about credit inquiries with credit granted would address concerns about the currently misleading nature of inquiry information: see Ch 52.

possible. The unwillingness of credit providers to report current credit provider status under the current credit reporting provisions serves as an undesirable precedent. As noted above, credit providers generally support the principle of reciprocity in credit reporting and obligations consistently to report information. The ALRC does not believe, however, that it is an appropriate role for regulation to mandate reporting obligations. Credit providers themselves and their industry associations should take responsibility for deciding how information sharing should proceed within the framework provided by legislation.

51.168 The United Kingdom provides one model in this regard. In the United Kingdom, the finance industry established the Steering Committee on Reciprocity (SCOR) to develop guidelines on the 'use and sharing of credit performance and related data on individuals'. This body consists of representatives from credit providers and credit reference agencies and has produced principles of reciprocity that set out the 'rules for the recording, supply and access of credit performance data' shared through the credit reporting agencies.[215]

51.169 As discussed in Chapter 50, the ALRC proposes that credit reporting agencies and credit providers should develop an industry code dealing with operational matters. This industry code should provide for access to information on credit information files according to principles of reciprocity (see Proposal 51–2 below).

51.170 Submissions emphasised the need to review and improve the existing regime of privacy protection, regardless of whether more comprehensive credit reporting is permitted by legislation or implemented by the finance the industry. For example, Nigel Waters of the Cyberspace Law and Policy Centre UNSW submitted:

> Any review of the existing rules inevitably invites questions about each stage of the information life cycle—collection, retention, access, use and disclosure—the answers to which straddle the boundary between negative and positive information.
>
> It is already the case that credit information files are permitted to contain some information that is not necessarily 'negative' such as current credit providers and inquiries, including type and amount of credit sought … The fact that the existing scheme is already a 'hybrid' strengthens the case for the review to address the issues surrounding comprehensive reporting at the same time as the need for changes to Part IIIA and the Code.[216]

51.171 The ALRC agrees with this approach. The ALRC's proposal to permit an extension in the categories of personal information that may be collected for credit reporting purposes is intended as part of broader reform of the credit reporting system.

---

215 Steering Committee on Reciprocity, *Information Sharing: Principles of Reciprocity* (2003).
216 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

51.172 Other changes to the regulation of credit reporting proposed in Chapters 52–55 are intended, among other things, expressly to prohibit the use or disclosure of credit reporting information in direct marketing, promote consistency and accuracy in the reporting of overdue payments, and improve complaint handling and dispute resolution processes.

51.173 The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* provide for review after operation for five years. The review should focus on the impact of more comprehensive credit reporting on privacy and the credit market.

Proposal 51–1 The proposed *Privacy (Credit Reporting Information) Regulations* should permit the inclusion in credit reporting files of the following categories of personal information in addition to those currently permitted under s 18E of the *Privacy Act*:

(a) the type of each current credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each current credit account was opened;

(c) the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and

(d) the date on which each credit account was closed.

Proposal 51–2 The credit reporting industry code (see Proposal 50–11) should provide for access to information on credit information files according to principles of reciprocity. That is, in general, credit providers only should have access to the same categories of personal information that they provide to the credit reporting agency.

Proposal 51–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for a review after five years of operation. The review should focus on the impact of more comprehensive credit reporting on privacy and the credit market.

52. Collection of Credit Reporting Information

Contents

Introduction 1445
Collection and notification 1446
Permitted content of credit information files 1447
Identifying particulars 1447
Inquiry information 1449
'Negative' information 1451
Publicly available information 1460
Compulsory reporting of permitted content 1462
Prohibited content 1464
Debts of children and young people 1465
Notification of collection 1468

Introduction

52.1 As discussed in Chapter 50, the ALRC proposes that the credit reporting provisions of the *Privacy Act 1988* (Cth) be repealed and credit reporting regulated under the general provisions of the *Privacy Act* and the proposed Unified Privacy Principles (UPPs).[1] Privacy rules imposing obligations on credit reporting agencies and credit providers should be promulgated in regulations made under the *Privacy Act*—the proposed *Privacy (Credit Reporting Information) Regulations*.

52.2 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act* dealing with the collection (and notification of collection) of information in credit information files and credit reports and makes proposals on how these matters should be dealt with under the proposed UPPs and *Privacy (Credit Reporting Information) Regulations*.

52.3 The issues in this chapter and Chapters 53–55 are discussed broadly in the order of the proposed UPPs, which are intended to replace the Information Privacy Principles and National Privacy Principles (NPPs). Where applicable, the provisions of the UPPs and Part IIIA of the *Privacy Act* are briefly compared.

---

1 See Part D.

Collection and notification

52.4 The proposed 'Collection' principle in the UPPs provides that an agency or organisation may only collect personal information:

- that it reasonably believes the information is necessary for one or more of its functions or activities;
- by lawful and fair means and not in an unreasonably intrusive way;
- about an individual only from that individual, if it is reasonable and practicable to do so; and
- in compliance with the 'Specific Notification' principle.

52.5 The proposed 'Specific Notification' principle in the UPPs provides that at or before the time an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

- fact and circumstances of collection (for example, how, when and from where the information was collected);
- identity and contact details of the agency or organisation;
- fact that the individual is able to gain access to the information;
- purposes for which the information is collected;
- main consequences of not providing the information;
- types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and
- avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

52.6 Where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of the above matters and the source of the information, if requested by the individual.

52.7 The provisions of Part IIIA depart significantly from these principles (and the equivalent NPP) in two relevant respects. First, s 18E of the *Privacy Act* sets out the

permitted content of credit information files held by credit reporting agencies,[2] and no other personal information may be included in an individual's credit information files, even if the information is 'necessary' in terms of the privacy principles.

52.8 Secondly, Part IIIA contains a specific notification obligation in that, under s 18E(8)(c), a credit provider must not give to a credit reporting agency personal information relating to an individual if 'the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency'.

52.9 Issues relating to the permitted content of credit information files and notification of the collection of personal information in credit reporting are discussed below.

Permitted content of credit information files

52.10 The permitted content of credit information files and credit reports has been subject to a range of comment and criticism. This is discussed below, with the exception of the specific issue of more comprehensive reporting, which was discussed in Chapter 51.

Identifying particulars

52.11 A credit information file may contain information that is 'reasonably necessary … to identify the individual'.[3] Under s 18E(3), the Privacy Commissioner has determined that credit information files may contain: an individual's full name, including any known aliases, sex, and date of birth; a maximum of three addresses consisting of a current or last known address and two immediately previous addresses; name of current or last known employer; and driver's licence number.[4]

52.12 The identifying particulars permitted in credit information files are important in several contexts, including in relation to the accuracy of credit reporting (because identifiers are used to match records) and the value of credit reporting information for non-credit related purposes, such as identity verification.[5] These issues are discussed in Chapters 53 and 54.

Identity theft

52.13 In the Issues Paper, *Review of Privacy—Credit Reporting Provisions* (IP 32), the ALRC asked whether credit reporting regulation should provide expressly for the

---

2 The permitted content of credit information files is summarised in Ch 49.

3 *Privacy Act 1988* (Cth) s 18E(1)(a).

4 Privacy Commissioner, *Determination under the Privacy Act 1988: 1991 No 2 (s 18E(3)): Concerning Identifying Particulars Permitted to be Included in a Credit Information File*, 11 September 1991.

5 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

problem of identity theft—the theft or assumption by a person of the pre-existing identity of another person.[6] For example, credit reports might be permitted to contain information that the individual concerned has been the subject of identity theft.[7]

52.14 In the United States, under the *Fair Credit Reporting Act 1970* (US), an individual may, in defined circumstances, require that a credit reporting agency insert a 'fraud alert' on a credit information file. A fraud alert is a statement that notifies prospective users of a credit report that the individual concerned 'may be a victim of fraud, including identity theft'.[8] Credit reports in the United Kingdom are also permitted to indicate that the individual has been the subject of identity theft.[9]

52.15 This suggestion received considerable support in submissions.[10] Legal Aid Queensland expressed concern that where an individual is the victim of identity theft, there is currently no centralised system for dealing with this.[11] The Australian Privacy Foundation noted that the ability to 'flag' identity theft seems 'both in the interests of consumers, and directly relevant to the primary purpose of credit assessment'.[12]

52.16 Some submissions in favour of including notations relevant to identity fraud stated that such information should only be recorded on the initiative of the individual who has been the subject of identity theft.[13] The Consumer Action Law Centre submitted that regulation should require that the alert be given to any credit provider who accesses information in that credit information file.[14]

52.17 The Australian Finance Conference (AFC) noted that, in some jurisdictions,[15] legislation allows for the issue of a court certificate to a victim of identity crime.[16]

---

6 See Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006), 15.

7 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–23.

8 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) § 1681c–1.

9 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

10 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007.

11 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

12 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

13 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

14 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

15 *Criminal Law (Sentencing) Act 1988* (SA) s 54; *Criminal Code* (Qld) s 408D.

16 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

Such a certificate, which may be issued at the court's own initiative or on application by either the victim or the prosecutor,

> is not a remedy. It does not compel others to take restorative action, eg for financial institutions to reinstate a person's credit rating. Rather the certificate provides a means to present the outcome of a court's decision in a way that may be used by the victim.[17]

52.18 There is concern that identity theft is becoming more prevalent due to developments in information and communications technology. The ALRC agrees that there is merit in the credit reporting provisions being amended, on the request of the individual, to allow notations to be placed on an individual's file in relation to identity theft.

Proposal 52–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.

Inquiry information

52.19 A credit information file may include information that is a record of both a credit provider having sought a credit report in relation to a credit application and the amount of credit sought in the application.[18] In addition, the *Credit Reporting Code of Conduct* states that 'a general indication of the nature the credit being sought' may also be included.[19]

52.20 In IP 32, the ALRC noted concerns expressed about the listing of this 'inquiry' information.[20] For example, the Consumer Credit Legal Centre (NSW) Inc (CCLC) has stated that 'the listing of inquiries on credit reports is completely ambiguous and misleading for credit providers in relation to the assessment of credit'.

> In our advice and casework experience, it is becoming increasingly common for a person's application for credit to be rejected solely on the basis of the number of inquiries on the person's credit report, despite there being no default listings. Worse, it is arguable that consumers are being penalised for shopping around.[21]

---

17 Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, *Discussion Paper—Identity Crime* (2007), 28.

18 *Privacy Act 1988* (Cth) s 18E(1)(b)(i).

19 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [1.1].

20 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.17].

21 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

52.21 Submissions continued to express concern about the role of inquiry information in credit risk assessment.[22] Consumer credit caseworkers related their experiences about individual clients being unfairly declined credit on the basis of multiple inquiry listings, including due to 'shopping around' for credit cards or frequent changes of telecommunications service provider.[23]

52.22 The CCLC conceded that consumers with more than a specified frequency of inquiries on their credit report are statistically more likely to default in the future than those who have less than a specified frequency. This is because, for example, a series of applications for personal loans within a short time often precedes bankruptcy. However, the CCLC stated that reliance on this statistical construct

> will inevitably disadvantage consumers who have multiple inquiries for completely different reasons. For example, there is absolutely no evidence to suggest a nexus between bankruptcy and mobile phone applications.[24]

52.23 The CCLC submitted that inquiry information relating to services (such as telecommunications) should only appear 'as an audit trail' and not be used in credit risk assessment.[25] The Australian Privacy Foundation submitted that there should be a requirement on credit providers not to use inquiry information 'negatively' in credit risk assessment without establishing the reason for the inquiries.[26] The Office of the Privacy Commissioner (OPC) stated that the ALRC should consider whether to allow credit information files to record that a credit offer has been accepted, in relation to a specific inquiry, without the amount being specified.[27]

52.24 The CCLC submitted that, if the permitted content of credit reporting is to include information about current credit commitments, inquiry information should not be available to credit providers, 'only to the person the report concerns and any authorised auditing body'.[28]

52.25 In Chapter 51, the ALRC proposes that a limited form of more comprehensive credit reporting should be permitted, which would allow credit granted to be matched with inquiry information. This reform should mean that inquiry information will no longer be as open to misinterpretation or relied on to the same extent in credit scoring

---

22 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; L Lucas, *Submission PR 95,* 15 January 2007.

23 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 85–89.

24 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 86.

25 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 10.

26 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

27 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

28 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 11.

processes. The ALRC would welcome further comment on the role of inquiry information under the more comprehensive credit reporting scheme proposed by it and whether any other reform relating to the collection, use or disclosure of inquiry information is desirable.

'Negative' information

52.26 The permitted content of credit information files and credit reports includes a range of 'negative' information. Submissions raised a number of concerns about permitted content in relation to small overdue payments; dishonoured cheques; bankruptcy and similar information; and serious credit infringements.

Small overdue payments

52.27 Section 18E(1)(b)(vi) permits the inclusion in credit information files of information about credit where the individual is at least 60 days overdue in making a payment and the credit provider has taken steps towards recovery of the amount outstanding. The credit reporting provisions do not provide for any minimum amount for debts that may be listed, except in the case of presented and dishonoured cheques (discussed below). The ALRC understands, however, that telecommunications providers and other credit providers have agreed not to list overdue payments of less than $100.[29]

52.28 In IP 32, the ALRC noted concerns about aspects of the listing of small debts, including by telecommunications companies.[30] In particular, there were concerns that the consequences of listing a small debt far outweigh the gravity of the conduct—especially as many small debts are said to be related to problems with billings systems, billing errors and change of address notification.[31] For example, the Telecommunications Industry Ombudsman (TIO) stated that common scenarios from its complaint handling experience are where:

- the default relates to an amount that was accrued after the consumer claims to have cancelled the service;
- the consumer claims never to have received a bill for the amount in question (often due to change of address);
- the default relates to an old debt, of which the customer either was not aware, or believed that the amount had either been paid or waived in resolution of a complaint;
- the consumer claims the debt does not belong to them (mistaken identity).[32]

---

29 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Optus, *Submission PR 258,* 16 March 2007.

30 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.11]–[5.15].

31 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

32 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

52.29 There was support for a limit on the minimum amount of overdue payments listed by credit reporting agencies.[33] Legal Aid Queensland suggested that imposing a minimum listing amount of $500 across all credit providers is 'fairer and more easily implemented than giving credit providers differing levels of access'.[34] The OPC also suggested that the ALRC should consider the introduction of a statutory minimum listing amount of $500.[35] The TIO stated that it

> has received complaints where consumers have been default listed for amounts as low as $37. In such cases, a default listing seems entirely disproportionate to the quantum of the debt. While the TIO does not have a definitive view on the precise dollar limit that should be imposed, a limit in the order of $500 does not appear unreasonable.[36]

52.30 The extent to which small debts are predictive of future default is relevant to the desirability of imposing a minimum amount for the listing of overdue payments. In this context, the ALRC referred to the results of research conducted by Dun and Bradstreet focusing on telecommunications debts, which claimed to show that individuals who default on low value amounts (below $500) or non-bank credit are at higher risk of defaulting on larger amounts provided under more traditional credit arrangements.[37] In its submission, Dun and Bradstreet stated that there should be no minimum limits on listing debts.[38]

52.31 Nigel Waters of the Cyberspace Law and Policy Centre UNSW cast doubt on the application of the Dun and Bradstreet research to Australia, and stated that:

> Even if there was a similar correlation in Australia it does not follow that allowing the use of this information is justified, given the significant consequences for individuals of a 'default' record.[39]

52.32 In contrast, credit providers were in no doubt about the significance of small debts in relation to credit risk assessment and considered that there should be no limit on the minimum amount, or no limit lower than $100.[40] The AFC stated:

---

33 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

34 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

35 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007. Other submissions also suggested a $500 minimum: Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 14; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

36 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

37 Dun & Bradstreet Australasia, 'Low Value Defaults are a High Risk Equation' (2006) 5 *Consumer Credit Reporting* 2.

38 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

39 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

40 Confidential, *Submission PR 297,* 1 June 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007; AAPT Ltd, *Submission PR 260,* 20 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007.

> Imposing a minimum default listing as a means of addressing a perceived lack of compliance or misuse of the credit referencing system by a few would, in our view, not be appropriate or warranted and would impact on the system to the detriment of the other participants, including all customers (existing and future) of credit.[41]

52.33 AAPT commented that, while it accepted that there are 'commercial practicalities involved in not chasing debts of less than $100, the ability to default list for $100 should be re-considered'.[42]

52.34 There is, therefore, no consensus between industry and consumer groups about the benefits and problems involved in reporting small debts. Veda Advantage currently operates an agreed minimum of $100 and credit providers generally do not object to such a limit (if only because small debts may not justify the cost of listing). The AFC submitted that a 'market driven setting of a minimum as a matter of commercial practice is preferable to a prescribed minimum' because it provides the 'requisite flexibility to react to the market in a timely fashion while maintaining the integrity of the credit referencing system and appropriate protections for the individual and credit providers'.[43]

52.35 Some of the problems caused by the listing of small debts can be addressed by other mechanisms, such as improved data quality and complaint-handling processes. On the other hand, there remains significant support for the imposition of a minimum amount by regulation. Another alternative would be to leave the question to self-regulation by credit providers and credit reporting agencies, with consumer group input.

Proposal 52–2 Credit reporting agencies only should be permitted to list overdue payments of more than a minimum amount.

Question 52–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide a minimum amount for overdue payments listed by credit reporting agencies? If not, by what mechanism should a minimum amount for overdue payments be set and enforced?

---

41 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

42 AAPT Ltd, *Submission PR 260,* 20 March 2007. EnergyAustralia noted the importance of reporting small debts as a debt collection tool: EnergyAustralia, *Submission PR 229,* 9 March 2007.

43 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

Overdue payments and capacity to repay

52.36 Credit providers have legal obligations, including under the uniform *Consumer Credit Code*,[44] not to provide credit where capacity to repay has not been reasonably established. There have been suggestions that where a credit provider improperly extends credit beyond an individual's capacity to repay, no adverse listing should be made (or remain) on the individual's credit information file.[45]

52.37 The Banking and Financial Services Ombudsman (BFSO) submitted that credit reporting regulation should require credit providers (in the case of a disputed listing) to show that consumers had the capacity to repay the listed debt at the time that credit was extended; and provide that the credit provider is not entitled to list an outstanding debt where a consumer negotiates a variation[46] or is being assisted by a bank,[47] unless the consumer fails to adhere to any subsequent arrangement.[48]

52.38 The Australian Privacy Foundation and Nigel Waters recognised the policy importance of promoting responsible lending practices but stated that

> it is difficult to justify excluding any actual defaults (over a sensible monetary threshold) from 'permitted content' of [credit information files] given that they are clearly relevant to an individual's capacity to repay other loans.[49]

52.39 The ALRC tends to agree with this view and does not propose any change to credit reporting regulation in this regard.

Dishonoured cheques

52.40 Section s 18E(1)(b)(vii) permits the listing on credit information files of information that is a record of a twice presented and dishonoured cheque for an amount of not less than $100. Questions may be raised about the appropriateness of this provision, as there is some doubt about whether a dishonoured cheque constitutes 'credit' as that term is defined for the purposes of Part IIIA.

---

44 The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories. Under s 70 of the *Consumer Credit Code* , a court may reopen an unjust transaction. In determining whether a transaction is unjust the court may have regard to, among other things, whether 'the credit provider knew, or could have ascertained by reasonable inquiry of the debtor at the time, that the debtor could not pay': *Consumer Credit Code* s 70(2)(l).

45 Banking and Financial Services Ombudsman, *Submission in Response to the Consumer Affairs Victoria Issues Paper: Consumer Credit Review*, 1 July 2005. This suggestion was supported by: Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007. The suggestion was opposed by Optus, on the basis that telecommunications service providers have no obligation to assess capacity to repay: Optus, *Submission PR 258,* 16 March 2007.

46 Under the *Consumer Credit Code* s 66.

47 In accordance with the *Code of Banking Practice*: Australian Bankers Association, *Code of Banking Practice* (1993) cl 25.2.

48 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

49 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

52.41 The OPC stated that the ALRC should consider removing the ability to list dishonoured cheques.[50] This course was also favoured by the Australian Privacy Foundation and Nigel Waters.[51] Waters stated:

> If it were determined, and widely known, that dishonoured cheques are 'credit', there is the potential for almost any individual or organisation to be a 'credit provider' and gain access to [credit information files]. This would allow a major expansion of consumer credit reporting well beyond the relatively constrained limits, and beyond the policy objectives of the legislation.[52]

52.42 The ALRC understands that, in practice, dishonoured cheques are rarely listed with credit reporting agencies. The ALRC tends to agree that the listing of presented and dishonoured cheques is anomalous and should no longer be permitted. The ALRC would, however, welcome further comment on this issue.

Proposal 52–3 The proposed *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques, as currently permitted under s 18E(1)(b)(vii) of the *Privacy Act*.

Personal insolvency information

52.43 Section 18E(1)(b)(ix) permits the inclusion in credit information files of information about 'bankruptcy orders made against the individual'. The Act does not define the term 'bankruptcy order' and the term is not used in bankruptcy legislation.

52.44 Under the *Bankruptcy Act 1966* (Cth), a person may become bankrupt upon the making of a sequestration order by the Federal Court following the presentation of a creditors' petition.[53] However, bankruptcy does not always require the making of an 'order against an individual'. For example, bankruptcy can occur following the acceptance of a debtors' petition by the Official Receiver.[54] The *Bankruptcy Act* also provides, as alternatives to bankruptcy, debt agreements under Part IX and personal insolvency agreements under Part X.

52.45 In IP 32, the ALRC suggested that the fact that the term 'bankruptcy order' is not defined in the *Privacy Act* creates uncertainty about what may or may not be listed. The ALRC asked for comments on whether the application of Part IIIA of the *Privacy*

---

50 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
51 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.
52 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007
53 See *Bankruptcy Act 1966* (Cth) pt IV, s 43(2).
54 See Ibid pt IV, s 55(4A).

Act to information about bankruptcy and agreements under the *Bankruptcy Act*, as used in s 18E(1)(b)(ix), should be clarified.[55]

52.46 The suggestion that the term 'bankruptcy order' be clarified received support in submissions.[56] The Insolvency and Trustee Service Australia (ITSA) stated that, in practice, credit reporting agencies and credit providers interpret this term as including voluntary arrangements under Part IX and Part X, as well as bankruptcy proper. ITSA suggested, nevertheless, that 'personal insolvency information included in a person's credit information file needs to be aligned with a person's insolvency status under the *Bankruptcy Act*'.[57]

52.47 Some submissions stated that credit reports should be able to include all personal insolvency information.[58] The Consumer Action Law Centre submitted that the *Privacy Act* be clarified 'to provide for separate categories of listings for the different types of bankruptcy and for Part IX and Part X agreements'.[59] The OPC suggested that 'to promote consistency and reduce complexity' consideration should be given to whether information about Part IX and Part X agreements should be permitted content of a credit information file.[60]

52.48 The CCLC expressed concern about the listing of debt agreements under Part IX of the *Bankruptcy Act* and submitted that such listings, if permitted, should be removed when the debtor has satisfied their obligations under the agreement.[61]

52.49 The Government has specifically asked ITSA to address the question of whether the fact that a debtor has entered into a debt agreement under the *Bankruptcy Act* should be included in credit information files. The arguments against reporting debt agreements include that debtors should be encouraged to enter into debt agreements and an incentive for doing so is that some of the public 'stigma' of personal insolvency will be ameliorated. On the other hand:

> A debt agreement can be used only by a debtor who is insolvent and is a formal insolvency administration under the bankruptcy legislation which allows the debtor's

---

55 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.20].

56 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Insolvency and Trustee Service Australia, *Submission PR 235,* 12 March 2007.

57 Insolvency and Trustee Service Australia, *Submission PR 235,* 12 March 2007.

58 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007.

59 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

60 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

61 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 34.

> debts to be compromised. This means creditors are paid less than the full amount of their debts and this information should be available to all creditors in the future.[62]

52.50 ITSA concluded that the 'policy reasons which support the public notification of bankruptcy … apply equally to debt agreements' and that if one aim of credit reporting is to ensure that 'fewer persons face financial difficulties' then reporting of debt agreements should be supported.[63]

52.51 ITSA has concerns about the accuracy and completeness of personal insolvency information recorded on credit reports. ITSA stated that:

> It is unclear if credit reporting agencies are including all relevant information as a 'bankruptcy order' to accurately determine a person's insolvency status. For example, because there is no definition of that term, credit reporting agencies are at liberty to include or not include notices of objections made under the *Bankruptcy Act*.[64]

52.52 In ITSA's view, there is uncertainty about whether not including the notice of objection is a breach of the credit reporting provisions. ITSA submitted that ensuring that credit reporting information about a person's insolvency status aligns with their status under the *Bankruptcy Act* is an important factor in ensuring the accuracy of credit reporting.[65]

52.53 Clearly, the term 'bankruptcy orders' does not reflect all the types of personal insolvency administration available under the *Bankruptcy Act*. ITSA has noted that, in addition to bankruptcies, including voluntary debtor's petitions and deceased estates administered in bankruptcy, the *Bankruptcy Act* provides for voluntary arrangements with creditors under Part IX and Part X and post-bankruptcy administration.[66]

52.54 All these forms of administration are currently recorded on the National Personal Insolvency Index (NPII),[67] the source of bankruptcy information collected by credit reporting agencies.[68] Information on the NPII is publicly available information.

---

62 Insolvency and Trustee Service Australia, *Submission PR 235,* 12 March 2007.

63 Ibid.

64 A bankrupt subject to a notice of objection is not discharged from bankruptcy and the absence of such information inaccurately reflects the person's insolvency status: Ibid.

65 Ibid.

66 See, *Bankruptcy Act 1966* (Cth) pt VI, div 6.

67 The NPII is established and maintained in accordance with the *Bankruptcy Regulations 1996* (Cth) pt 13.

68 The content of searches on the NPII will ordinarily show: type of administration or proceeding; date of administration or proceeding; identification number; full name and alias of debtor; address of debtor; date of birth of debtor; occupation and business name of debtor; name of trustee or controlling trustee; particulars of any prior or subsequent listing; the end date of the administration: Insolvency and Trustee Service Australia, *National Personal Insolvency Index* (2007) <www.itsa.gov.au> at 1 August 2007.

52.55 The AFC referred to an increase in the incidence of Part IX Debt Agreements.[69] While the AFC recognised that 'a debt agreement has different connotations to a bankruptcy order insofar as it reflects a different attitude of a customer towards the repayment of their debt', it recommended that

> either the definition of bankruptcy order be amended or a new definition of Part IX & Part X information be included in the Act to clarify that debt agreement and Part X personal insolvency agreement information can be included on a customer's credit information file.[70]

52.56 The ALRC considers that credit reporting information should be permitted to include all categories of information available on the NPII. Such information is important in credit risk assessment and, in practice, credit providers rely on obtaining this from credit reporting agencies rather than directly from the NPII.[71] In accordance with their obligations to ensure the accuracy and completeness of credit reporting information, credit reporting agencies should ensure that credit reports adequately differentiate the forms of administration identified on the NPII.

Proposal 52–4 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index (NPII) administered under the *Bankruptcy Regulations 1966* (Cth).

Proposal 52–5 Credit reporting agencies, in accordance with obligations to ensure the accuracy and completeness of credit reporting information, should ensure that credit reports adequately differentiate the forms of administration identified on the NPII.

Serious credit infringements

52.57 Section 18E(1)(b)(x) permits the inclusion in credit information files of the 'opinion of a credit provider that the individual has … committed a serious credit infringement'. A serious credit infringement is defined as an act done by a person:

> (a) that involves fraudulently obtaining credit, or attempting fraudulently to obtain credit; or
>
> (b) that involves fraudulently evading the person's obligations in relation to credit, or attempting fraudulently to evade those obligations; or

69 Approximately 6,500 new debt agreements were made between 1 July 2006 and 30 June 2007, compared with just under 5,000 debt agreements in the 2005–06 financial year: P Ruddock (Attorney-General), 'Amendments to Support Debt Agreements Commence' (Press Release, 9 July 2007).

70 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

71 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

> (c) that a reasonable person would consider indicates an intention, on the part of the first-mentioned person, no longer to comply with the first-mentioned person's obligations in relation to credit.[72]

52.58 A serious credit infringement listing has more serious consequences for the individual concerned than other default listings—not least because such a listing may remain on the record for seven years, as compared to five years for most other adverse information.

52.59 For an overdue payment to be listed on a credit information file, an individual must be 60 days overdue in making a payment, and the credit provider must have taken recovery action.[73] There are no similar requirements for the listing of a serious credit infringement.

52.60 The *Credit Reporting Code of Conduct* provides some guidance on what constitutes a serious credit infringement.[74] The ALRC noted, however, that it may be appropriate for the credit reporting provisions to define what constitutes a serious credit infringement with more precision—rather than leaving it to differing interpretations under the internal policies of credit providers.[75]

52.61 There was broad support in submissions for clarification of the meaning of a serious credit infringement.[76] For example, National Legal Aid stated that the definition has proved to be too loosely drafted.

> A range of actions or failures to act where the individual concerned had no intention of avoiding their obligations are characterised as serious credit infringements. The definition is regularly applied to anyone who fails to advise a forwarding address when leaving a property with an amount owing to a utility provider.[77]

52.62 There was no clear view on how the issue should be dealt with. For example, the CCLC submitted that a series of steps, including the giving of notices and the making of reasonable attempts to contact the individual, should be taken before a serious credit

---

72 *Privacy Act 1988* (Cth) s 6(1).
73 Ibid s 18E(1)(vi).
74 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [62]–[65].
75 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.24].
76 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 29; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.
77 National Legal Aid, *Submission PR 265,* 23 March 2007.

infringement listing is made.[78] The CCLC also recommended that there should be a 'separate process for other types of fraudulent conduct, requiring a conviction in a criminal court before a listing can be made, and the reference to fraud should be deleted from the current serious credit infringement section'.[79] The BFSO stated that a serious credit infringement should only be listed where fraud has been proven.[80] The practice of listing individuals who cannot be found by a credit provider ('clearouts') as having committed a serious credit infringement without further confirmation was also criticised.[81]

52.63 The ALRC recognises that there are valid concerns about the interpretation of the current definition of a serious credit infringement. The definition appears too broad. The ALRC would welcome further comments on whether a definition of serious credit infringement should be retained in the credit reporting regulations and, if so, how it should be framed. For example, one possible approach would be to remove any equivalent of paragraph (c) of the existing definition—restricting the concept of a serious credit infringement to situations where there are reasonable grounds for suspicion of fraud.

Question 52–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow for the listing of a 'serious credit infringement' or similar and, if so, how should this concept be defined?

Publicly available information

52.64 The credit reporting provisions regulate some aspects of the collection of publicly available information, but not others. The definition of a 'credit reporting business' excludes businesses or undertakings that maintain records 'in which the only personal information relating to individuals is publicly available information'.[82] On the other hand, the permissible content of a credit information file does not include 'publicly available information'—although some permissible items may be publicly available, such as bankruptcy and court judgment information.

52.65 The appropriateness of regulating some categories of publicly available information under Part IIIA, but not others, may be questioned. For example, if a credit reporting agency holds publicly available information about court judgments in

78 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 29–30.

79 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 31.

80 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

81 See, eg, Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

82 *Privacy Act 1988* (Cth) s 6(1). Part IIIA provides that credit reporting agencies and credit providers may disclose information contained in a record 'in which the only personal information relating to individuals is publicly available information': see, *Privacy Act 1988* (Cth) ss 18K(1)(k), 18N(9) definition of 'report'.

separate records—rather than in credit information files—the information can be retained indefinitely as there are no specified time limits for retention under general privacy principles. If governed by Part IIIA, the information would have to be deleted five years after the judgment was made.[83]

52.66 In IP 32, the ALRC asked what issues are raised by the collection of publicly available personal information for use in credit reporting and how should the collection, use and disclosure of such information be regulated.[84]

52.67 The OPC recommended that the definition of a 'credit reporting business' be amended to remove the exclusion for publicly available information and noted that this

> will have the effect of regulating publicly available personal information, such as commercial credit information, including defaults, directorships, judgments and proprietorship information that is collected by a credit reporting agency for the purpose of assessing an individual's eligibility for credit.[85]

52.68 The OPC stated that, if such a proposal were to proceed, the permitted content of a credit information file should be amended to include publicly available information.[86]

52.69 There is much support from credit reporting agencies and credit providers for the inclusion of new categories of publicly available information in credit information files and credit reports, including for identity verification (discussed below) and in order to ensure the data quality of credit reporting information.[87]

52.70 There is also some criticism of the collection of existing categories of publicly available information permitted under s 18E. As discussed, these include concerns about the collection of bankruptcy and other personal insolvency information. In addition, the CCLC noted concerns about the listing of court judgments:

> Court judgments are not necessarily an indicator of a person's credit worthiness, but rather, disputes that have been determined by the courts … Further in cases where a consumer is appropriately insured, his or her insurance company may opt to initiate or defend proceedings in the consumers' name under their right of subrogation. It would be manifestly unjust for the consumers' ability to obtain credit to be jeopardised in these circumstances.[88]

---

83 *Privacy Act 1988* (Cth) s 18F(2)(e).

84 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–26.

85 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

86 Ibid.

87 See Ch 54.

88 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 32.

52.71 The CCLC submitted that court judgments should only be included 'if they relate to a credit contract by a credit provider as defined by the *Privacy Act* or any other relevant instrument'.[89] The ALRC notes that where court judgment information is not relevant to credit worthiness, the collection of the information could be challenged on the basis that it breaches the proposed 'Data Quality' principle of the UPPs, which requires that personal information be 'relevant' with reference to a permitted purpose of collection.

52.72 The current provisions dealing with the collection of publicly available information create undesirable inconsistency and a lack of clarity. In practice, credit reporting agencies are important aggregators of publicly available information. The ALRC understands that they comply with the credit reporting provisions by ensuring that publicly available information is kept in separate databases and is not technically provided as part of a credit report.

52.73 The ALRC considers that the interests of individuals and business would be better served if publicly available information were permitted content under the *Privacy (Credit Reporting Information) Regulations*. This would ensure that where publicly available information is used in credit risk assessment, privacy interests are fully protected by, for example, the application of the special rights of access and correction that apply to credit reporting information and complaint-handling mechanisms.

Proposal 52–6 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information.

Compulsory reporting of permitted content

52.74 A related issue is whether it should be compulsory for credit providers to report some or all kinds of information that may be included in a credit information file. At present, there are no obligations placed on credit providers to report information to credit reporting agencies.

52.75 The value of credit information files in the assessment of credit worthiness may be reduced significantly by the fact that credit providers may 'pick and choose' whether information about particular overdue payments or other adverse information is reported. It has been suggested, therefore, that it should be made compulsory for credit providers to report negative information.[90] On the other hand, compulsory reporting obligations may interfere with the relationship between a credit provider and its

89 Ibid, rec 32.

90 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 63.

customers, for example, when negotiating a repayment plan with an overcommitted individual.

52.76 In IP 32, the ALRC asked whether credit providers that subscribe to a credit reporting agency should be required to provide to the credit reporting agency some or all kinds of information that may be included in a credit information file.[91]

52.77 In submissions, some credit providers supported compulsory reporting as desirable, but not necessarily as a subject appropriate for regulation.[92] Westpac, for example, supported compulsory reporting, in addition to new standards governing the format and timing of reporting, in order to 'improve the accuracy of credit information files and therefore optimise credit assessments'. This would also 'provide more certainty for the consumer as to how their data will be reported'.[93]

52.78 Other submissions from industry opposed compulsory reporting because of possible compliance costs for smaller credit providers[94] and telecommunications service providers.[95] One bank noted that compulsory reporting

> would need to somehow accommodate the often extraordinary circumstances that surround consumer credit defaults. These include death, divorce and other extreme health issues.

52.79 Legal Aid Queensland supported the compulsory reporting of current credit provider status[96] and identifying particulars, but not default information. Legal Aid Queensland stated that

> negotiating repayment arrangements often takes longer than the 60 days.[97] If the borrower is disputing liability 60 days is an insufficient timeframe in which to come to a settlement of the dispute.[98]

52.80 The BFSO noted that compulsory reporting, by removing discretion on the part of credit providers in relation to listing, would diminish the effectiveness of important provisions of the *Code of Banking Practice*, which requires a subscribing bank to try to

---

91 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–2.

92 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Westpac, *Submission PR 256,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007; National Credit Union Association Inc, *Submission PR 226,* 9 March 2007.

93 Westpac, *Submission PR 256,* 16 March 2007.

94 Min-it Software, *Submission PR 236,* 13 March 2007.

95 Optus, *Submission PR 258,* 16 March 2007.

96 *Privacy Act 1988* (Cth) s 18E(1)(b)(v).

97 That is, the period after which overdue payment information may be reported under Ibid s 18E(1)(b)(vi).

98 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

help customers overcome difficulties with credit.[99] In strongly opposing compulsory reporting, the Consumer Action Law Centre stated:

> The market is able to determine at what point the cost of providing more information outweighs the benefits of having more information in the credit reporting system. The proposal to implement compulsory reporting would be a complete inversion of the purpose of the regulatory scheme by using it to advance the interests of certain market participants who have been unable to get the market to justify these interests. It would be the worst sort of regulation—imposing red tape on business to protect the interests of certain industry players.[100]

52.81 Submissions also considered that, if reporting was compulsory, there would need to be improvement in the provisions regulating the use and disclosure of credit information for non-credit related purposes,[101] in dispute resolution processes,[102] and compliance with responsible lending obligations.[103]

52.82 This issue is related to the discussion in Chapter 51, about the desirable model of more comprehensive reporting. In that context, there is broad support for the concept of reciprocity—which includes the idea that credit providers should contribute to the credit reporting agency data of the categories the credit provider receives from the agency. This principle, however, need not rule out some discretion on the part of credit providers with respect to reporting information about individual customers, in certain circumstances. The ALRC considers that, like reciprocity, the question of compulsory reporting should be a matter for self-regulation by credit providers and their industry associations.

Prohibited content

52.83 Section 18E(2) provides that certain types of personal information must never be included in an individual's credit information file. This list is similar to, but differs in some respects from, the general definition of 'sensitive information' in s 6(1). The OPC suggested that the ALRC consider whether the definition of prohibited content set out in s 18E(2) should be aligned with the definition of sensitive information in s 6(1) of the *Privacy Act*.[104]

52.84 The definitions of prohibited content and sensitive information serve quite distinct purposes. The former, in effect, acts to prohibit collection (with or without the consent of the individual); the latter to restrict collection without consent, and use or

---

99 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007. Optus made a similar point in relation to the *Telecommunications Credit Management Code of Practice*: Optus, *Submission PR 258,* 16 March 2007.

100 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

101 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

102 Queensland Law Society, *Submission PR 286,* 20 April 2007.

103 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

104 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

disclosure for secondary purposes.[105] Nevertheless, it may make sense to align the two definitions, if only to simplify the drafting of the Act.

52.85 Two significant issues arise. First, the definition of 'sensitive information' includes 'health information'. Health information is defined in s 6(1) to include information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual …

52.86 It is conceivable that some content of credit information files permitted under s 18E may constitute health information in terms of s 6(1)—for example, a record of an overdue payment owed to a hospital or doctor. Credit reporting information, however, would not ordinarily be specific enough to constitute information 'about' the individual's health (as opposed to about the fact an individual owes money to a health service provider). In any case, credit providers, unless exempt, are already bound by the NPPs in addition to their obligations under Part IIIA, so aligning the definitions would not cause any new problem in this regard.

52.87 Secondly, the definition of prohibited content in Part IIIA includes personal information recording an individual's 'lifestyle, character or reputation'.[106] While this may be seen as an important protection against the inclusion of subjective opinions in credit reporting information, such information also would not be permitted content under the *Privacy (Credit Reporting Information) Regulations*.

Proposal 52–7 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as that term is defined in s 6(1) of the *Privacy Act*.

Debts of children and young people

52.88 In IP 32, the ALRC noted concerns about credit information files and credit reports concerning individuals under the age of 18—especially in relation to the listing of debts by telecommunication companies in relation to mobile telephone contracts.[107]

105 In conjunction with NPPs 10 and 2.1.

106 *Privacy Act 1988* (Cth) s 18E(2)(f).

107 See Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.141]–[5.147].

52.89 A 'protective' approach is reflected in the common law, where contracts are not binding on a person under the age of 18 unless it is a contract for 'necessaries'. The common law applies in all Australian states and territories except New South Wales, where legislation has modified the common law position and focuses on the contract being for the 'benefit' of the child or young person, where the child or young person is sufficiently mature to understand his or her participation in the contract.[108]

52.90 While many companies are mindful of how the law of contract applies to those under the age of 18—and many mobile telephone contracts are signed by adults on behalf of young people—young people, nevertheless, regularly purchase mobile telephones in their own name or sign contracts for future telecommunications services in their own name.[109] Other young people may enter contracts with banks or other financial institutions for loans or credit cards. While some seek loans or credit facilities due to the need to live independently, others may complete offers for credit cards inadvertently sent to them as part of a marketing campaign. Other young people may accumulate a debt by not paying a fine, such as parking fines, or fines issued for public transport ticket violations.

52.91 Where credit obligations are not discharged, telecommunications companies and other credit providers may list overdue payment information with a credit reporting agency. Such information can remain on the individual's credit information file for up to five years and prejudice a young person's future access to credit. This may be the case even where the legality of the contract is in question.

52.92 In IP 32, the ALRC asked what issues are raised by credit information files and credit reports about children and young people, and how the handling of this information should be regulated.[110]

52.93 Some submissions stated that the collection of credit reporting information about individuals under the age of 18 should be prohibited.[111] For example, the Consumer Action Law Centre stated

---

108 *Minors (Property and Contracts) Act 1970* (NSW). Some limited exceptions to the common law apply in the other states and territories: see L Blackman, *Representing Children and Young People: A Lawyers Practice Guide* (2002), 240.

109 A 1999 Australian study indicated that 48% of young people under the age of 18 with a mobile telephone signed the contract in their own name: A Funston and K MacNeill, *Mobile Matters: Young People and Mobile Phones* (1999) Communications Law Centre, 3. Note, however, that in 2005 most telecommunications companies commenced using a new form of contract requiring disclosure of age and not allowing persons under the age of 18 to sign the contract in their own name: Children and Young People Issues Roundtable, *Consultation PC 121*, Sydney, 7 March 2007.

110 See Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–24.

111 National Legal Aid, *Submission PR 265,* 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007. Except in the case of unpaid fines: Min-it Software, *Submission PR 236,* 13 March 2007.

> no listings [should] be permitted while the individual remains under the age of 18, in recognition of the different capacities and experience of young people. If debts incurred by a minor are to continue to be allowed to be listed, we would strongly advocate that such listings (and other listings related to minors) be subject to a shorter timeframe before deletion, for example two years, in recognition of the different legal position of minors.[112]

52.94 In contrast, the Institute of Mercantile Agents (IMA) noted that its members 'encounter many instances of young persons lying in order to obtain a mobile phone, internet access and credit cards'.

> Given these circumstances it is difficult to justify requiring some special case method for handling identifier and credit based information relating to young persons. Our industry members are aware of cases where a number of creditors have been deliberately targeted by young consumers who appear to be aware that nothing will be done to them for their fraudulent activities.[113]

52.95 Questions may be raised about whether any person under the age of 18 has the developmental capacity to consider the long term consequences of these decisions.[114] Decisions regarding consumer credit can have a long term impact if the young person is then unable to meet the commitments and is listed as a credit risk. The effect may not be immediate, but may have repercussions some years later when the young person is in need of credit. One approach would be to permit the collection of credit reporting information about individuals under the age of 18, but to require deletion after the expiry of a shorter maximum permissible period than applies to other default information.

52.96 On balance, the ALRC proposes that the collection in credit reporting information about individuals under the age of 18 years should be prohibited. Any regulation to this effect, however, would have to recognise that credit providers may not always know the age of their clients. The ALRC is interested also in comment on whether such a reform might have some undesirable effects, for example in prejudicing the ability of some younger people—living independently, or those with parents with bad credit records—to obtain credit or services they need.

---

112 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; The OPC also submitted that shorter credit listing timeframes should be considered for minors: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

113 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

114 New South Wales Commission for Children and Young People, *Consultation PC 34*, Sydney, 18 July 2006.

Proposal 52–8 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information about individuals the credit provider or credit reporting agency knows to be under the age of 18 years.

Notification of collection

52.97 The proposed 'Specific Notification' principle provides that, at or before the time an organisation collects personal information, the organisation must take reasonable steps to ensure that the individual is aware of a range of matters including the fact and circumstances of collection (for example, how, when and from where the information was collected); the identity and contact details of the agency or organisation; the types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

52.98 Part IIIA provides only indirectly for notification. Under s 18E(8)(c), a credit provider must not give to a credit reporting agency personal information relating to an individual if 'the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a credit reporting agency'.

52.99 In IP 32, the ALRC noted that the words 'at the time of, or before, acquiring the information' may permit the credit provider a choice about when to provide notice to the individual that information may be disclosed. It was suggested that, given that a significant period may elapse between the relevant events, more prescriptive notice provisions may be appropriate.

52.100 The ALRC asked what issues are raised by the provisions of the *Privacy Act* requiring individuals to be informed about the disclosure of personal information to a credit reporting agency and about how these provisions operate in practice.[115]

52.101 Submissions from a range of bodies favoured the imposition of more prescriptive notice requirements.[116] As discussed below, these included suggestions

115 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.30], Question 5–3.

116 Queensland Law Society, *Submission PR 286,* 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Westpac, *Submission PR 256,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

that credit providers or credit reporting agencies should specifically be required to notify individuals about default listings and complaint-handling processes.[117]

52.102 The interpretation of s 18E(8)(c) is the subject of a representative complaint to the OPC, lodged in April 2006 by the CCLC and the Consumer Credit Legal Service Inc (Vic) against Baycorp Advantage Business Information Services Ltd and Alliance Factoring Pty Ltd.[118] The complaint relates to the listing of about 600,000 individuals for default or serious credit infringement, lodged by Alliance in relation to Telstra debts.

52.103 The complaint claims a failure to inform individuals that personal information might be disclosed to a credit reporting agency. The complainants submitted that the correct interpretation of s 18E(8)(c) is that an individual should be notified at the time of, or before, the handing over of personal information, and the relevant time is the time of the application for a loan, account or other relevant facility. The opposing argument is that a credit provider may comply with s 18E(8)(c) by notifying an individual that it intends shortly to list a default—and does not need to have notified the individual about this possibility at the time of the initial credit application.

52.104 The Consumer Action Law Centre contested the validity of the latter interpretation, which it considered 'has been developed to meet the interests of debt purchase firms and [credit reporting agencies] to maximise the listing of utility defaults'.[119] The Centre submitted that, nevertheless,

> more prescriptive notice provisions may be appropriate, as they would in effect simply clarify the operation of the existing provision, namely that notice should be given at relevant times, for example at initial application stage, if a default is to be listed, if a debt is assigned and so on.[120]

52.105 The OPC noted that the notice provision in s 18E(8)(c) is important as it 'promotes transparency between the individuals, credit providers and to some extent credit reporting agencies'. The notice provision was said to generate a number of complaints, particularly in relation to assigned loans where, for example, notice may have been given a long time before a listing is made, or an assignee assumes notice has been provided by the original credit provider and does not provide notice at the time of listing.[121] The OPC recommended that s 18E(8)(c) be re-drafted to 'align it more

---

117 Issues concerning the notification given when an individual's application for credit is refused on the basis of a credit report under *Privacy Act 1988* (Cth) s 18M are discussed in Ch 52.

118 The outcome of this complaint is pending.

119 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

120 Ibid.

121 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

closely with the requirements under NPP 1.3, and to require that notice is given prior to any listing being made or a debt being assigned'.[122]

52.106 Other submissions also favoured imposing an express obligation on credit providers, or credit reporting agencies, to notify individuals about the collection or proposed collection of credit reporting information at specified times or in specified circumstances (in addition to notification at the time of the initial credit application).

52.107 The most common suggestions were that credit providers should be required to notify individuals before or at the time of listing a default or other adverse credit reporting information;[123] or when a debt is assigned.[124] For example, the CCLC recommended that credit providers should be required to issue a notice giving individuals 30 days to rectify a default, or raise a dispute, before a default can be reported.[125] The BFSO stated:

> It would be useful if there was a more explicit regulatory requirement in either the Act or the Code requiring a credit provider to notify a consumer as part of the debt collection process that it intends to list a debt on the consumer's credit information file and the time frame.[126]

52.108 Such a requirement was opposed by others. EnergyAustralia referred to the practical difficulties involved in notifying individuals who leave no forwarding address.[127] Min-it Software stated that an 'obligation to notify individuals when adverse information is added to their file highlights a lack of commercial reality'.[128]

52.109 Submissions also focused on the obligations of credit reporting agencies,[129] including to ensure that individuals are notified about adverse listings and can seek correction of any inaccurate information. The OPC submitted that the ALRC should

---

122 Ibid.

123 Queensland Law Society, *Submission PR 286,* 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Westpac, *Submission PR 256,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 7; Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007.

124 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007.

125 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 7.

126 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

127 EnergyAustralia, *Submission PR 229,* 9 March 2007.

128 Min-it Software, *Submission PR 236,* 13 March 2007. Min-it Software, nevertheless, favoured notification prior to the default listing of an assigned debt.

129 Queensland Law Society, *Submission PR 286,* 20 April 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

consider whether credit reporting agencies should be required to inform an individual within 14 days when an adverse listing is made.[130] The BFSO stated:

> Ideally, the credit reporting agency would notify the individual each time a default or serious credit infringement listing is made or altered, including when any publicly available information such as a court order or bankruptcy is added to the credit information file.[131]

52.110 Nigel Waters submitted that credit reporting agencies should have an obligation to inform individuals periodically of the existence of their consumer information file and, specifically, at the time a default listing is made. Waters noted that, while these requirements might appear onerous, 'the contribution that pro-active notification would make to data quality should more than outweigh the cost'.[132] Queensland Law Society members also referred to the data quality benefits of notification and noted that email may provide a cost-effective means of notification.[133]

ALRC's view

52.111 Section 18E(8)(c) has been the subject of varying interpretation and lacks clarity in its application. For example, the drafting allows credit providers to argue that the obligation does not require:

- notification at the time of the initial credit application that a default might be listed in the future; or

- notification before or at the time a default listing is made, provided that notification (that a default might be listed in the future) was given at the time of the initial credit application.[134]

52.112 More prescriptive notice provisions seem appropriate, if only to bring the credit reporting provisions in line with the proposed 'Specific Notification' principle. In relation to notification at the time of the initial application, the *Privacy (Credit Reporting Information) Regulations* should be drafted in a form consistent with the proposed 'Specific Notification' principle and the approach to privacy notices discussed in Chapter 21.

---

130 The OPC also stated that there should be notification of any other listing which may have an adverse impact, such as file linking: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

131 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

132 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007. Also Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

133 Queensland Law Society, *Submission PR 286,* 20 April 2007.

134 The ALRC understands that giving notice immediately prior to listing a default has been adopted generally as good industry practice: Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

52.113 In addition, the *Privacy (Credit Reporting Information) Regulations* should prescribe the circumstances in which a credit provider must later inform an individual that personal information might be disclosed to a credit reporting agency. These circumstances should include where 'negative' credit reporting information is to be reported.[135]

52.114 The ALRC is interested in further comment on whether credit reporting agencies should be required to notify individuals when such information is reported to them by credit providers. Credit reporting agencies already offer, for a fee, to notify individuals of additions or changes to their credit information files.[136] Veda Advantage has advised that it intends to pursue a capacity to manage consumer 'notifications electronically and directly with consumers where appropriate'.[137]

Proposal 52–9 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, at or before the time credit reporting information is collected about an individual, credit providers must take reasonable steps to ensure that the individual is aware of:

(a) the fact and circumstances of collection (for example, how and where the information was collected);

(b) the credit provider's and credit reporting agency's identity and contact details;

(c) the fact that the individual is able to gain access to the information;

(d) the main consequences of not providing the information;

(e) the types of people, organisations, agencies or other entities to whom the credit provider and credit reporting agency usually discloses credit reporting information; and

(f) the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her credit reporting information.

135 That is, the information referred to in *Privacy Act 1988* (Cth) s 18E(1)((vi)–(x), to the extent these are permitted content under the proposed new *Privacy (Credit Reporting Information) Regulations*.

136 See Ch 55.

137 Veda Advantage, *Submission PR 272,* 29 March 2007.

Proposal 52–10 The proposed *Privacy (Credit Reporting Information) Regulations* should prescribe the specific circumstances in which a credit provider must inform an individual that personal information might be disclosed to a credit reporting agency, for example, in circumstances where the individual defaults in making payments.

Question 52–3 In what specific circumstances should a credit provider be obliged to inform an individual that personal information might be disclosed to a credit reporting agency; and what information should notices contain? Who should give notice when a debt is assigned—the original credit provider, the assignee or both?

Question 52–4 Should the proposed *Privacy (Credit Reporting Information) Regulations* prescribe specific circumstances in which a credit reporting agency must inform an individual that it has collected personal information?

53. Use and Disclosure of Credit Reporting Information

Contents

Introduction 1475
Use and disclosure 1475
Comparing Part IIIA and the NPPs 1477
Use and disclosure of credit reporting information 1478
Internal credit management 1481
Mortgage and trade insurers 1482
Debt collection 1483
Direct marketing 1487
Identity verification 1490
Disclosure of reports relating to credit worthiness 1495
Consent and credit reporting 1497
Consent to disclosure of information 1498
Disclosure to a credit reporting agency 1498
'Bundled' and 'true' consent in credit reporting 1499
Consent and notification 1500

Introduction

53.1 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act* dealing with the use and disclosure of information in credit information files and credit reports and makes proposals on how these matters should be dealt with under the proposed Unified Privacy Principles (UPPs) and the *Privacy (Credit Reporting Information) Regulations*. The chapter also considers the role of consent in the regulation of credit reporting system.

Use and disclosure

53.2 Under the proposed 'Use and Disclosure' principle in the UPPs, an agency or organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

> (a) both of the following apply:
>
> > (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

> (ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or
>
> (b) the individual has consented to the use or disclosure; or
>
> (c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat …
>
> (d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
>
> (e) the use or disclosure is required or authorised by or under law; or
>
> (f) the agency or organisation reasonably believes that the use or disclosure is necessary for [law enforcement purposes].

53.3 The relative simplicity of the general principle set out in clause (a), which permits use or disclosure for a related secondary purposes within the reasonable expectation of the individual concerned, may be contrasted with the complexity of the use and disclosure provisions of Part IIIA.

53.4 Sections 18K, 18L, 18N, 18P and 18Q all deal with aspects of the use or disclosure of personal information (or both). These provisions place various limits on use and disclosure of personal information based on the identity of the person or organisation to whom information is disclosed; the source and nature of the information; and the purpose for which the information is to be used. Briefly, the use and disclosure provisions of Part IIIA deal with the following:

- s 18K places limits on the disclosure by credit reporting agencies of personal information contained in credit information files;
- s 18L places limits on the use by credit providers of personal information contained in credit reports;
- s 18N places limits on the disclosure by credit providers of personal information in 'reports relating to credit worthiness';
- s 18P places limits on the use or disclosure by mortgage insurers or trade insurers of personal information contained in credit reports; and
- s 18Q places limits on the use of personal information obtained from credit providers by: a corporation that is related to the credit provider; a corporation that proposes to use the information in connection with an assignment or purchase of debt; and a person who manages loans made by the credit provider.[1]

---

1 These provisions are summarised in more detail in Ch 49.

53.5 In sum, Part IIIA prescribes more than fifty different circumstances in which the use or disclosure of personal information is authorised. As the categories of permissible use and disclosure are exhaustive, all other use or disclosure of personal information covered by the ambit of the provisions is prohibited. Additional complexity arises because, in some instances, the provisions also limit the kinds of information that may be disclosed.[2]

53.6 Despite the extensive nature of these provisions, there may also be some gaps in their coverage. Notably, while the permitted contents of credit information files held by credit reporting agencies and the disclosure of personal information contained in those files are regulated in detail by ss 18E and 18L respectively, Part IIIA does not expressly limit the use of credit information files by credit reporting agencies.

Comparing Part IIIA and the NPPs

53.7 The Part IIIA provisions may operate to make use and disclosure of credit reporting information more or less restrictive than is the case under general privacy principles. The extent to which any particular category of use or disclosure permitted by Part IIIA would be permitted by the NPPs (or the proposed UPPs), however, is difficult to determine. The determination depends primarily on whether specific circumstances authorised by Part IIIA are related secondary purposes within the reasonable expectations of the individual.

53.8 The Issues Paper, *Review of Privacy—Credit Reporting Provisions* (IP 32) noted that how broadly an organisation can describe the primary purpose needs to be determined on a case-by-case basis and depends on the circumstances.[3] The OPC's *Guidelines to the National Privacy Principles* state that when an individual provides, and an organisation collects, personal information, they almost always do so for a particular purpose. This is 'the primary purpose of collection even if the organisation has some additional purposes in mind'.[4]

53.9 In IP 32, the ALRC stated that, even on a broad conception of the primary purpose, it is hard to argue that the disclosure of information by a credit provider to a credit reporting agency is for the primary purpose of collection. Disclosure does not directly serve purposes connected with the provision of finance by the credit provider to the particular individual. Rather, the information is disclosed so that it may be used

---

2 For example, s 18N(1)(be) permits the disclosure of personal information to a person or body supplying goods or services to an individual who intends to pay by credit card or electronic funds transfer. The information that may be disclosed is limited to information reasonably necessary to identify the individual, and as to whether the individual has access to funds sufficient to meet the payment concerned.

3 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.105]–[5.107], citing Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 35.

4 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 35.

in the future, including by other credit providers in assessing other loan applications. This conclusion has not been contested.

53.10 In IP 32, the ALRC noted that, for the same reasons, disclosure to a credit reporting agency is unlikely to be considered a related secondary purpose for the purposes of NPP 2.1(a). This conclusion was contested in submissions. Nigel Waters of the Cyberspace Law and Policy Centre stated:

> It is suggested that it may be necessary for credit providers to obtain consent for disclosures involved in the credit reporting system because they would not fit within the alternative exception for secondary purposes … I submit that it is at least arguable that within the context of the well established operation of the credit market, disclosure to [credit reporting agencies] and other [credit providers] is both a related purpose and within reasonable expectations (NPP 2.1(a)).[5]

53.11 These comments serve to highlight the fact that different conclusions can be reached even on the most basic questions about how NPP 2 applies to credit reporting information. In this context, the provisions of Part IIIA can be seen as providing some certainty for existing finance industry practices, removing the need to determine whether, for example, the disclosure by a credit provider of personal information to a credit reporting agency; a mortgage insurer; the assignee of a debt to the credit provider and so on, are within the reasonable expectations of the individual concerned.

Use and disclosure of credit reporting information

53.12 In IP 32, the ALRC asked a number of questions about the provisions of Part IIIA that regulate the use and disclosure of credit reporting information.[6] Submissions contained a number of general comments on regulating use and disclosure.

53.13 The Australasian Retail Credit Association (ARCA) noted that it has developed a 'governing principle' for the operation of the credit reporting system. The ARCA governing principle states:

> Data are shared only for the prevention of over-commitment, bad debt, fraud and to support debt recovery and debtor tracing, with the aim of promoting responsible lending.[7]

53.14 This governing principle was expressly supported by some other stakeholders.[8] In the context of support for a more comprehensive credit reporting system, Veda Advantage submitted that, based on the ARCA principle, the rules governing use and disclosure should provide:

---

5 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

6 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 5–9 to 5–11; 5–16.

7 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

8 Veda Advantage, *Submission PR 272,* 29 March 2007; American Express, *Submission PR 257,* 16 March 2007.

> The purpose of collection is the promotion of good credit management, and transparency of credit practices. This includes but is not limited to the prevention of over commitment, bad debt, and fraud; identity verification and to support debt recovery and debtor tracing.[9]

53.15 Veda Advantage and others[10] submitted that limits on the use and disclosure of credit reporting information should be more flexible, especially with regard to possible new uses of personal information. The IMA stated that the limits on disclosure by credit reporting agencies are 'tight and often misunderstood'. The Institute of Mercantile Agents (IMA) contended that all parts of the 'credit continuum' (of which debt collection was said to be a major part), should have access to credit files 'where a need can be substantiated'.[11]

53.16 As Veda noted, the use of credit reporting information in other jurisdictions extends beyond credit risk assessment and into areas such as 'insurance underwriting, employment, tenancy, and licensing'.

> Data users have found that attributes of an individual's credit file correlate with other behaviour—like insurance risk. Whilst these uses may or may not be considered appropriate, there is no mechanism under the current framework for the assessment of such 'novel' use.[12]

53.17 Because the 'benefit to society and consumers from novel uses of credit data cannot be predicted', Veda Advantage submitted that the regulatory environment 'needs to provide a mechanism which will allow for the assessment and facilitation of new uses of credit data—subject to appropriate harm minimisation processes'. Veda submitted:

> Regulators should have a mechanism under which data controllers can assess and approve new or novel use of credit data in the context of an approved Data Governance Standard.[13]

53.18 The implications of more comprehensive credit reporting for the existing use and disclosure limitations were considered in submissions. The OPC submitted that any change to the personal information permitted to be used in credit reports under a more comprehensive credit reporting system does not imply or necessitate 'any change to who may access this information'.

---

9 Veda Advantage, *Submission PR 272,* 29 March 2007.

10 Ibid; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

11 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

12 Veda Advantage, *Submission PR 272,* 29 March 2007. Veda stated that 'the use of credit information for identity verification is just one example of the use of third party collected credit data that is difficult to resolve within the current regulatory framework'. Identity verification is discussed in detail below.

13 Ibid. The 'data controller', in this context, would be the credit reporting agency itself. Data Governance Standards are described as 'binding, transparent and enforceable standards on the handling of data specific to an organisation', put in place by organisations and operating as a form of co-regulation similar to an industry code: Veda Advantage, *Submission PR 272,* 29 March 2007.

> Any system regulating credit reporting should limit the use and disclosure of personal credit information to that required to fulfil the purpose for which it was legally collected, unless the individual has given consent to further or alternate use of their personal credit information, or a use or disclosure is authorised or required by law.[14]

53.19 MasterCard Worldwide (MasterCard) noted that the additional information available under more comprehensive credit reporting means that 'permission to access the data should be limited and clearly defined'.[15] The OPC stated that 'as a general principle, only credit providers should be able to access information from credit information files unless there are cogent public interest reasons why other persons should'.[16]

53.20 Submissions also observed that credit reporting regulation could provide different levels of access to the information held by credit reporting agencies.[17] As stated by the Australian Privacy Foundation:

> The current regime includes a presumption that there is only a single level of access to consumer credit information files. We believe this is too simplistic. We submit that there needs to be a more nuanced debate about different levels of access: who needs access to what information for what purposes?[18]

ALRC's view

53.21 The use and disclosure of credit reporting information is potentially useful for a wide range of secondary purposes. Submissions provided detailed views in relation to specific use or disclosure of credit reporting information including, for example, internal credit management, mortgage and trade insurance, debt collection, law enforcement, direct marketing and identity verification. These views are discussed in more detail below.

53.22 As noted above, Part IIIA prescribes more than fifty different circumstances in which the use or disclosure of personal information is authorised; and the categories of permissible use and disclosure are exhaustive. It is hard to justify this level of prescription, which risks being overtaken by changes in credit industry practices.

53.23 The ALRC considers that there is room to simplify and consolidate the use and disclosure provisions of Part IIIA, for example, in relation to use and disclosure by

---

14 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

15 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

16 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007. In general, credit reporting agencies may disclose personal information contained in credit information files only to those persons who are 'credit providers', as that term is defined in the Act and OPC determinations: see Ch 49.

17 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007.

18 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. See, however, ss 18N(1)(be), 18N(1)(c).

credit reporting agencies and credit providers for the purposes of credit risk assessment;[19] securitisation;[20] or credit assessment of a guarantor.[21]

53.24 A process of consolidation will be necessary, in any case, as a result of the ALRC's proposal that there should be no equivalent in the *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act* (see Proposal 53–4 below). Some of the circumstances in which the disclosure of information by credit providers is expressly authorised by s 18N may need to be preserved in the regulations, but with application to a more circumscribed category of information.[22]

53.25 In the ALRC's opinion, there should be an additional category of permissible use and disclosure of credit reporting information incorporating, expressly or by reference, the secondary use provision in the proposed 'Use and Disclosure' principle. That is, in addition to the use and disclosure authorised specifically by the *Privacy (Credit Reporting Information) Regulations*, the regulations should provide that other related use or disclosure within the reasonable expectations of the individual concerned is permitted. This would not extend, however, to direct marketing purposes (see Proposal 53–3 below).

Proposal 53–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information, based on those uses and disclosures currently permitted under ss 18K, 18L and 18N of the *Privacy Act*.

Proposal 53–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, in addition, a credit reporting agency or credit provider may use or disclose credit reporting information for related secondary purposes, as permitted by the proposed 'Use and Disclosure' principle.

Internal credit management

53.26 Section 18L(ba) permits a credit provider to use a credit report or personal information derived from the report for 'the internal management purposes of the credit provider, being purposes directly related to the provision or management of loans by the credit provider'.

---

19 See, *Privacy Act 1988* (Cth) ss 18K(1)(a), 18L(1).
20 See, Ibid ss 18K(1)(ac), 18L(1)(aa)–(ab).
21 See, Ibid ss 18K(1)(c), 18L(1)(b).
22 That is, credit reporting information, rather than personal information related to credit worthiness as defined by s 18N(9)(b).

53.27 The CCLC expressed concern about s 18L(ba), stating that the provision is 'unnecessarily wide' and 'should be narrowed down so that both the consumer and the credit provider are clear on the exact circumstances in which a credit report can be accessed'.[23]

53.28 The ALRC notes that the credit provider must have already obtained the credit report for the purposes of assessing an application for credit.[24] Section 18L(ba) does not appear to allow credit providers to obtain new information from the credit reporting agency for internal credit management unless there is a current credit application (or a default).[25]

Mortgage and trade insurers

53.29 Part IIIA contains a number of provisions relating to the disclosure of credit reporting information to mortgage and trade insurers;[26] and the use and disclosure of credit reporting information by mortgage and trade insurers.[27] In particular, under ss 18K(1)(d) and (e), a credit reporting agency may disclose personal information contained in a credit information file to a mortgage or trade insurer.

53.30 The OPC suggested that there should be good public policy reasons for mortgage insurers and trade insurers to have direct access to credit reports when other types of insurers do not have direct access. The OPC observed:

> Most credit providers have some discretionary power to approve applications for mortgage insurance. However, where a loan proposal does not meet certain criteria and mortgage insurance is required, for example, where the borrowers are self employed, the mortgage insurer will complete their own assessment of the loan proposal. This involves a complete assessment by the mortgage insurer i.e. they require all the documentary evidence provided to the credit provider such as bank statements and income statements and also request a credit check to complete their assessment.[28]

53.31 The OPC submitted that the ALRC should consider whether mortgage and trade insurers should have limited access to and use of individuals' credit information files through credit providers.[29] That is, the credit reporting provisions could be amended to allow credit providers (but not credit reporting agencies) to disclose an individual's credit report to a mortgage or trade insurer, where access to the report is required to assist in the assessment of the individual's credit worthiness.

---

23 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.
24 That is, the credit report was obtained under *Privacy Act 1988* (Cth) s 18K(1)(a), (b) or (c).
25 That is, under Ibid s 18K(1)(f)–(g).
26 Ibid ss 18K(1)(d)–(e); 18N(1)(bb).
27 Ibid 18P.
28 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
29 Ibid.

53.32 The ALRC is interested in further comment on this idea and, in particular, on the possible effects on current commercial practices in the mortgage and trade insurance industries.

Question 53–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow credit providers (but not credit reporting agencies) to disclose an individual's credit reporting information to a mortgage or trade insurer, where access to the information is required to assist in the assessment of the individual's credit worthiness?

Debt collection

53.33 Credit providers may use credit reports to assist them in recovering overdue payments.[30] A credit provider, in this context, may include a debt collection agency that has purchased debts from a credit provider, or other assignee.

53.34 In addition, a credit provider may disclose certain items of personal information from a credit report to a debt collector for the purpose of collecting overdue payments. The information that may be disclosed is limited to identifying information about the individual; information about overdue payments; and information about court judgments and bankruptcy orders.[31]

53.35 In IP 32, the ALRC observed that mercantile agents and others engaged in debt collection and related activities have expressed concern that they are not permitted to obtain personal information on credit information files directly from credit reporting agencies (or to report information to them). This was said to hamper the ability of mercantile agents to locate debtors and, more generally, to assist small businesses in risk management.[32]

53.36 Where organisations engaged in debt collection do have direct access to the credit reporting system, other issues arise. These were said to include individuals being threatened with having a default listed as a 'collection tool'; the listing of defaults that are disputed by the individuals concerned or without proper notification; and the listing of individuals who are not able to be located as having committed a serious credit infringement.[33]

---

30 *Privacy Act 1988* (Cth) s 18K(1)(g) permits credit reporting agencies to disclose information to credit providers for this purpose.

31 Ibid s 18N(1)(c).

32 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.132].

33 Consumer Credit Legal Centre (NSW) Inc, *Report in Relation to Debt Collection* (2004), 62.

53.37 In IP 32, the ALRC asked what issues are raised by the use of the credit reporting system in debt collection and how the use of personal information contained in credit information files and credit reports for debt collection should be regulated.[34]

53.38 The IMA submitted that debt collectors should have direct access to credit information files, including overdue payment information; and be able to report and update information. More generally, the IMA noted that it operates in a commercial environment in which

> our industry is routinely the accounts receivable department of credit providers or alternatively now the assigned owner of debt as well concurrently being the debt collector for numerous clients … [35]

53.39 EnergyAustralia referred to the existing provisions of Part IIIA, which allow credit providers to disclose information to mercantile agents and stated that mercantile agents should be allowed to obtain this information directly from credit reporting agencies, rather than only through a credit provider.[36] Other submissions highlighted the need for direct access to the location information available on credit information files, particularly in the light of concerns about restrictions on access to other sources of location information, such as the electoral roll and other publicly available information.[37]

53.40 Other submissions considered that the debt collection provisions are appropriate, and there should be no direct access for debt collectors.[38] The OPC stated:

> In the case of mercantile agents, the Office is of the view that the current provision in s 18N(1)(c) of the Privacy Act is adequate as it permits a credit provider to disclose specific information from a credit information file (but not the credit file) to a mercantile agent for the purpose of collecting the specific debt that is owed. The restriction on access to an individual's credit information files for debt collection purposes in s 18N(1)(c) of the Privacy Act does not apply to debt collection activities carried out in-house by the credit provider.[39]

53.41 The OPC submitted, however, that mercantile agents that receive personal information from credit providers under the provisions of s 18N(1)(c) should be subject to a prohibition on the use and disclosure of that information for secondary purposes.[40]

---

34 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–21.

35 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.

36 EnergyAustralia, *Submission PR 229,* 9 March 2007.

37 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007. The operation of the *Privacy Act* in relation to publicly available information available in electronic form is discussed in Ch 8.

38 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

39 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

40 Ibid.

53.42 The Australian Privacy Foundation noted that, as the *Privacy Act* already provides for debt collectors to receive information from credit providers, direct access could only be for more general 'tracing' purposes.[41] The Consumer Action Law Centre also expressed concerns about assignees.

> In terms of assignees, we understand that access to credit information files is more appropriate as they effectively 'stand in the shoes' of the original credit provider, unlike contracted mercantile agents and collection firms. However, it should be remembered that, in practice, assignees use credit reporting information for debt collection purposes as assignment is, in effect, the outsourcing of debts and debt collection. For this reason, we suggest the Commission consider if assignees could be given more limited access to credit information files.[42]

53.43 Submissions raised ongoing problems in relation to credit reporting and debt collection practices.[43] The Telecommunications Industry Ombudsman (TIO) noted complaints in relation to telecommunications debt collection activity confirm that

> collection activity, which may include a default or threat of a default, continues even though the consumer disputes the debt in question. The TIO can advise anecdotally that we receive complaints where consumers claim that collection agents advise them to first pay any disputed amount to avoid a default listing and to subsequently attempt to resolve the dispute.[44]

53.44 Members of the Queensland Law Society expressed concern about the possible 'trawling' of credit reporting databases by debt collectors for identity and location information.[45] In relation to assignees, the Banking and Financial Services Ombudsman (BFSO) stated that:

> In our experience, problems can arise where a debt has been sold some years after the last contact between the credit provider and the individual, because the individual has moved address. An assignee may send a letter to last known address and then list either a default or serious credit infringement if there is no response. It appears, in some circumstances, that the listing is used as a way to 'draw out' the debtor, so that the debt can then be collected.[46]

53.45 Veda Advantage acknowledged that 'the threat of default listings as a primary means of, or in the absence of other debt collection activity is of great concern to consumers and their advocates'. Veda considered, however, that such concerns about the use of credit reporting information can be addressed by means other than restricting

---

41 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

42 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

43 Queensland Law Society, *Submission PR 286,* 20 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

44 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

45 Queensland Law Society, *Submission PR 286,* 20 April 2007.

46 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

access—including through credit reporting agency subscription agreements and rules of reciprocity.[47]

ALRC's view

53.46 The use and disclosure of credit reporting information in connection with debt collection is widely accepted as being one of primary purposes of the credit reporting system. Access to credit reporting for debt collection is, on some views, essential for the efficient functioning of the credit market.[48] Through credit reporting, credit providers share information necessary to locate debtors and are made aware of defaults to other credit providers.

53.47 Concerns about debt collection appear to arise mainly where debt collection activity is outsourced from the original credit provider to debt collection businesses, which may also become the assignees of the debt.[49]

53.48 Where debt collectors are not the assignees of the debt, access by them to credit reporting information can be obtained only through the credit provider. Many of the credit providers for whom IMA members act, however, are not subscribers to the credit reporting system. The ALRC understands that part of the reason the IMA has been lobbying for direct access to the credit reporting system is to service those businesses that, for reasons including size and resources, cannot participate in it directly.

53.49 There seems no compelling reason for change to the rules governing access to credit reporting information by debt collectors. In any case, the existing barriers to access are not necessarily regulatory. Access may be affected by commercial decisions made by credit reporting agencies in relation to terms and conditions of access, including decisions about fees and the quality of data likely to be provided by potential subscribers.

53.50 Many of the issues raised in submissions are already canvassed in guidance issued by the Australian Competition and Consumer Commission (ACCC) and the Australian Securities and Investment Commission (ASIC), who are jointly responsible for administering consumer protection legislation in relation to the debt collection industry.[50]

53.51 The *Debt Collection: Guideline for Collectors and Creditors* reflects the views of the ACCC and ASIC about how provisions of the *Trade Practices Act 1974* (Cth)

---

47 Veda Advantage, *Submission PR 272,* 29 March 2007.

48 Ibid.

49 Corporations are regarded as credit providers if they acquire the rights of a credit provider with respect to the repayment of a loan (whether by assignment, subrogation or other means): Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)*, 21 August 2006.

50 Australian Competition and Consumer Commission and Australian Securities and Investment Commission, *Debt Collection Guideline: For Collectors and Creditors* (2005).

and *Australian Securities and Investment Commission Act 2001* (Cth) apply to conduct in debt collection. In relation to credit reporting, the guidelines advise:

> [g] Do not state or imply that you intend to list a debt with a credit reporting service when:
>
> - you do not have a genuine belief that the debtor is liable for the debt;
> - you have no instructions to list the debt, and/or it is not your intention to do so;
> - listing is not permitted by law or under a mandatory code;
> - the debt has already been listed.
>
> [h] Equally, while it is appropriate to point out the possible consequences of a credit listing, you must not make misleading representations about those consequences.
>
> [i] Generally, it is not appropriate to make an adverse credit listing:
>
> - when you are in the process of investigating a debtor's claim that a debt is not owed;
> - if you are aware that the debtor has filed process with a tribunal or court disputing liability for the debt.[51]

53.52 It may not be effective or appropriate for the *Privacy (Credit Reporting Information) Regulations* to deal with issues that primarily concern debt collection practices. Debt collection practices that involve credit reporting are, however, related to broader concerns about data quality, which are discussed in Chapter 54. For example, consistent reporting of defaults, governed by industry protocols, would lessen the opportunity for debt collectors to threaten listing in order to obtain payment.

Direct marketing

53.53 Direct marketing involves the promotion and sale of goods and services directly to consumers. The application of privacy principles to direct marketing is discussed in more detail in Chapter 23. The proposed 'Direct Marketing' principle in the UPPs permits personal information to be used in direct marketing with consent or where it is impracticable for the organisation to seek the individual's consent and the organisation otherwise complies with the requirement of the principle. In contrast, Part IIIA does not permit the use or disclosure of personal information for the purpose of direct marketing, with or without the consent of the individual concerned.

53.54 Those opposed to more comprehensive credit reporting have highlighted concerns that it brings the risk that 'such comprehensive, centralised databases may be mined for data by credit providers and other reporting agencies for marketing

---

51 Ibid, Guideline 19[g]–[i].

purposes'.[52] Concerns about the possible use by competitors of credit providers' customer lists may also have been a brake on the existing credit reporting system.[53]

53.55 GE Capital Finance Australasia (GE Money), a proponent of more comprehensive reporting, noted that the perceived risk of smaller credit providers or new entrants to the credit marketing 'cherry picking' good customers directly from credit reporting agency lists was one reason for an initial lack of support for more comprehensive reporting in the United Kingdom.[54]

53.56 In submissions, proponents of more comprehensive credit reporting emphasised the need to maintain restrictions on the use or disclosure of credit reporting information for direct marketing,[55] at least in relation to 'positive' data.[56]

53.57 On the other hand, there was support for the idea that credit providers should be able to use credit reports to 'exclude' individuals from direct marketing offers to increase credit limits or refinance loans (pre-screening).[57] Dun and Bradstreet stated '[m]aking this a permissible use would be a significant step towards an environment in which unaffordable and unsustainable credit was not offered'.[58] MasterCard noted the importance in the credit card industry of decisions to extend credit limits and submitted that:

> As is current practice, credit report information should be accessible for *excluding* individuals from credit increase offers … It should be noted that this is very different from using credit reports to identify individuals for marketing purposes who should be approached to be offered additional credit. MasterCard opposes the selling of credit information for proactive marketing.[59]

53.58 Some submissions expressly opposed the use of credit reporting information in pre-screening.[60] The Australian Privacy Foundation stated that the experience of consumer organisations in this area is that many credit providers 'use any additional information they can acquire to increase the total volume of offers, inevitably leading

---

52 Westpac, *Submission PR 256,* 16 March 2007.

53 That is, in relation to credit providers' reluctance to report current credit provider status under *Privacy Act 1988* (Cth) s 18E(1)(b)(v).

54 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007. For this reason, GE Money favoured a prohibition on the use of 'positive' data in marketing.

55 Confidential, *Submission PR 297,* 1 June 2007; American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

56 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

57 American Express, *Submission PR 257,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

58 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.

59 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

60 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

to at least some inappropriate offers and to some excessive or unconscionable lending'.[61]

ALRC's view

53.59 Submissions and consultations indicated broad agreement that credit reporting regulation should ensure that credit reporting information is not able to be used for direct marketing. There appear to be different views, however, on what constitutes direct marketing and support among credit reporting agencies and credit providers for pre-screening of credit offers.

53.60 It has been argued that pre-screening is permissible under Part IIIA because, where a credit provider's information is simply 'cleaned' against credit reporting agency information, there is no use or disclosure of personal information (by the credit provider) or disclosure (by the credit reporting agency). Others consider that Part IIIA does not permit the pre-screening of lists.

53.61 The ALRC questions whether there is a significant difference between the use of credit reporting information for pre-screening and for direct marketing. It may be observed that, given individuals may have several current credit providers, the potential for marketing credit, if credit providers can 'pre-screen' using credit reporting information, is significant.

53.62 The ALRC considers that the *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information in direct marketing. There seems no compelling reason why such a prohibition should not extend to pre-screening lists by credit providers. The ALRC would, however, welcome further comment on this point.

Proposal 53–3 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing.

Question 53–2 Should credit providers be permitted to use credit reporting information to 'pre-screen' credit offers? If so, should credit providers be required to allow individuals to opt out, or should credit providers only be permitted to engage in pre-screening if the individual in question has expressly opted in to receiving credit offers?

61 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

Identity verification

53.63 In IP 32, the ALRC noted the potential use of credit reporting information in identity verification. Credit providers and other businesses have statutory obligations to verify the identity of their customers, including under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (the AML/CTF Act).[62]

53.64 The AML/CTF Act covers the financial sector, gambling sector, bullion dealers and other professionals or businesses ('reporting entities') that provide particular 'designated services'. The Act imposes a number of obligations on reporting entities when they provide designated services. These include obligations with respect to customer identification and verification of identity, record-keeping, establishing and maintaining an AML/CTF program, and ongoing customer due diligence and reporting.

53.65 The customer identification procedures required of reporting entities are set out in Part B of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (the AML/CTF Rules). For example, with respect to individuals and where the money laundering and terrorism financing risk is medium or lower, the AML/CTF Rules provide for an 'electronic-based safe harbour procedure'.[63]

53.66 In brief, this 'safe harbour' (in terms of compliance with the AML/CTF Rules) is available to reporting entities if they collect the customer's full name; the customer's date of birth; the customer's residential address; and verify:

(a) the customer's name and the customer's residential address using reliable and independent electronic data from at least two separate data sources; and either

(b) the customer's date of birth using reliable and independent electronic data from at least one data source; or

(c) that the customer has a transaction history for at least the past 3 years.[64]

53.67 One obvious source of electronic data in this context is credit reporting information held by credit reporting agencies. The use and disclosure of credit reporting information for these purposes, however, is not authorised by Part IIIA of the *Privacy Act*. Sections 18K and 18L place detailed limits on the disclosure of personal information by credit reporting agencies and use by credit providers respectively, and make no express provision for identity verification. The fact that credit reporting information might be used in electronic identity verification that complies with the AML/CTF Act is not sufficient to render disclosure for this purpose by a credit

---

62 The AML/CTF Act and its relationship with the *Privacy Act* is also discussed in Ch 13. Identity verification may also be required under other legislation such as the *Telecommunications Act 1997* (Cth): see, eg, Australian Communications and Media Authority, *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*.

63 See, *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1) 2007* (Cth) pt 4.2, [4.2.12]–[4.2.13].

64 See, Ibid pt 4.2, [4.2.13].

reporting agency 'required or authorised by or under law' for the purposes of Part IIIA.[65]

53.68 A related issue concerns anti-fraud services provided by businesses that maintain databases of personal information provided on credit and similar application forms that have been identified as suspicious. These databases are used to compare details on new credit applications (such as name, address and drivers' licence numbers) with those from previous suspect applications and provide a report back to the credit provider. IP 32 noted that these anti-fraud services may constitute a 'credit reporting business' for the purposes of Part IIIA—but this may not be widely appreciated.[66]

53.69 In IP 32, the ALRC asked what issues are raised by the possible use of credit information files for electronic identification and verification and how the use of credit information files for these purposes should be regulated.[67]

53.70 A number of stakeholders submitted that the *Privacy Act* or the AML/CTF Act should be amended to provide for the use and disclosure of credit reporting information for identification verification or in preventing or detecting identity fraud.[68]

53.71 Abacus–Australian Mutuals (Abacus) stated that the AML/CTF regulator, the Australian Transaction Reports and Analysis Centre (AUSTRAC) has confirmed that access to credit reporting agency records for electronic identity verification is 'not possible due to prohibitions contained in the Privacy Act 1988 and the status of the AML/CTF Rules as subordinate legislation'. Abacus submitted that, in light of this, an exception to allow the use of the credit reporting system may be warranted.[69]

53.72 ING Bank submitted that in order to facilitate the safe harbour contained in the AML/CTF Rules, the *Privacy Act* should be amended to allow the disclosure by a credit reporting agency, and the use by a credit provider, of credit reports in identity verification.[70] ING Bank noted that consumer credit reports are used to verify identity in the United States and the United Kingdom.

---

65 *Privacy Act 1988* (Cth) s 18K(1)(m).

66 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [7.45].

67 Ibid, Question 5–22; 5–23.

68 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; ING Bank, *Submission PR 230,* 9 March 2007; Experian Asia Pacific, *Submission PR 228,* 9 March 2007; Abacus–Australian Mutuals, *Submission PR 174,* 6 February 2007; Veda Advantage, *Submission PR 163,* 31 January 2007.

69 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

70 ING Bank, *Submission PR 230,* 9 March 2007.

> One of the advantages of electronic verification is the ability to use several data sources to create a match. Information contained within the credit bureau is a critical data source as it provides a source to strengthen the match of a customer's identity through confirmation of date of birth and transaction history.[71]

53.73 Veda Advantage stated that electronic identity verification has been a significant focus of attention in the development of the AML/CTF Act and that the use of credit reporting information for identity verification has a clear public benefit in protecting consumers and business from harm. The company sought 'urgent measures to permit the use of credit reporting data in electronic verification for the purposes of AML/CTF laws'. In this context, Veda noted that it has developed 'a data process using public number directory, electoral roll and credit information to perform real time electronic identity verification'.[72]

53.74 The role of more comprehensive credit reporting in addressing identity verification and related issues was highlighted by GE Money, which submitted that it would 'greatly enhance credit providers' ability to detect and prevent money laundering and fraudulent activities'.[73] Others have also suggested that more comprehensive reporting may 'enable identity fraud to be detected sooner, due to improved information flows'.[74]

53.75 There is support from credit reporting agencies and credit providers for the inclusion of new categories of publicly available information in credit information files and credit reports, including for identity verification and the prevention of identity fraud. For example, it has been suggested that credit reporting agencies should be able to collect information from the electoral roll[75] and state government births, deaths and marriages registries in order to combat identity fraud.[76]

53.76 GE Money submitted that, under a more comprehensive credit reporting system, credit reporting agencies should collect more 'application form or demographic data items'—which GE Money referred to as 'extended credit application summary' (ECAS) data.

> The list of ECAS data items should be unconstrained by legislation (other than by it being fit for money-laundering or fraud prevention purposes by way of comparison to previous applications) … [77]

53.77 It was suggested that ECAS data should include at least the following items: time with employer; time with the relevant credit provider; date of birth; drivers'

---

71 Ibid.
72 Veda Advantage, *Submission PR 272,* 29 March 2007.
73 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.
74 Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006), 8.
75 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.
76 P Switzer, 'Identity Crisis' (2006) (January) *Charter* 1. Information in state births, deaths and marriages registries is not made publicly available until the expiry of certain periods prescribed by legislation.
77 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

licence number; number of dependents; home and work telephone numbers; time at previous address and residential status.[78]

53.78 Other submissions opposed the use or disclosure of credit reporting information for electronic identity verification,[79] or considered that any proposal to permit such use or disclosure would be premature.[80] The OPC stated that

> expansion into activities such as identification verification by credit reporting agencies would appear to be a type of 'function-creep'. The Attorney General at the time the credit reporting provisions were introduced into the *Privacy Act* highlighted the need to limit what information is allowed to be held under the credit reporting provisions. The rejection of comprehensive credit reporting by the Attorney General at the time was seen as a way of avoiding 'function-creep' arising.[81]

53.79 The Australian Privacy Foundation and Nigel Waters submitted that this issue needs to be discussed more widely, as part of broader concerns about identity management, before any proposal is made. The Australian Privacy Foundation stated that identity verification and credit reporting needs to be approached

> in the wider context of developments such as the proposed Document Verification Service, the due-diligence requirements of financial services legislation including the AML-CTF Act 2006 and similar statutory identification obligations such as under the *Telecommunications Act 1997*. No express provision should be made for credit information files to be used for identification outside the credit reporting context pending the outcome of those wider discussions.[82]

ALRC's view

53.80 The ALRC recognises the force of arguments in favour of allowing credit reporting information to be used and disclosed for identity verification and related purposes. Credit providers are concerned that, while new statutory identity verification obligations have been imposed under the AML/CTF Act, they are not authorised to obtain electronic data that would enable them to comply efficiently. In particular, the ALRC understands that credit reporting information is potentially an important source of date of birth, which is not generally available from public sector databases.

53.81 On the other hand, the AML/CTF Rules provide considerable flexibility with regard to the means of identity verification. Verification of information collected about

---

78 Ibid. See, also Australian Finance Conference, *Submission PR 294,* 18 May 2007.

79 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007.

80 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

81 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

82 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

a customer may be based on: reliable and independent documentation; reliable and independent electronic data; or a combination of these.[83]

53.82 A range of sources of information could be used potentially for electronic verification. These sources include those that are currently available, such as the electronic Whitepages telephone directory and registers maintained by ASIC; and those subject to regulation that acts to restrict use in electronic identity verification, such as the electoral rolls and the Integrated Public Number Database maintained by Telstra.

53.83 The use of credit reporting information for identity verification is not an entirely new idea. A credit report was worth 35 points under the 100 point identity verification test provided for under the *Financial Transaction Reports Act 1988* (Cth).[84] Such reports, however, were provided directly to institutions by the individuals concerned, with consent. The ALRC does not propose that the *Privacy (Credit Reporting Information) Regulations* prevent the disclosure by individuals of their own credit reporting information for identity verification purposes.

53.84 The use and disclosure of credit reporting information for identity verification would still constitute a significant 'function creep' and needs to be authorised specifically by legislation. There was opportunity during the legislative process that led to the enactment of the AML/CTF Act and the issuing of the AML/CTF Rules, to provide specific authorisation, but this was not done. Rather, the Government deferred consideration of the use and disclosure of credit reporting information for identity verification until after the completion of the ALRC's Inquiry.

53.85 There are arguments that, if existing electronic sources of personal information are insufficient to meet the needs of reporting entities, the Government, having imposed identity verification obligations, should look to facilitate access to government databases[85] before looking to private sector databases, such as those held by credit reporting agencies.

53.86 The ALRC needs more information about the risks, benefits and possible alternatives before making any recommendation that the use and disclosure of credit reporting information for identity verification should be authorised. The issue needs to be considered in the light of many recent developments, including the proposed Document Verification Service and the due diligence requirements of financial services legislation and other similar statutory identification obligations. Ultimately, however, the balance between privacy and the need to combat money-laundering and the

---

83 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1) 2007* (Cth) [4.2.7].

84 *Financial Transaction Reports Regulations 1990* (Cth) r 4(1)(v).

85 Including, for example, databases relating to the proposed access card. The Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 105 permits the disclosure of access card information to a person other than the individual concerned, if the individual consents to the disclosure.

financing of terrorism in this context is a policy decision. The following question is designed to assist the ALRC to formulate a recommendation in this regard.

Question 53–3 If the use and disclosure of credit reporting information for identity verification purposes is not authorised under the proposed *Privacy (Credit Reporting Information) Regulations*, what other sources of data might be used by credit providers to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and similar legislation? What are the advantages and disadvantages of the alternate sources of data?

Disclosure of reports relating to credit worthiness

53.87 Section 18N applies to information contained in 'reports relating to credit worthiness'. A 'report' is defined, for the purposes of the section, as

> (a) a credit report; or
>
> (b) …any other record or information, whether in a written, oral or other form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;
>
> but does not include a credit report or any other record or information in which the only personal information relating to individuals is publicly available information.[86]

53.88 Consequently, s 18N(9) protects a broader category of information than other provisions of Part IIIA, which protect information contained in a 'credit report' or 'credit information file'. For example, while the disclosure by a credit provider of this broader category of information is protected,[87] credit providers' obligations to ensure the accuracy and security of information under s 18G apply only to information in a credit report—that is, information provided by a credit reporting agency.

53.89 In IP 32, the ALRC asked for comments on the existing statutory limits on the disclosure by credit providers of personal information contained in reports relating to credit worthiness. In particular, the ALRC asked what issues are raised by the application of s 18N of the *Privacy Act* to 'reports' and whether information relating to credit worthiness that is not contained in a credit report should covered only by the NPPs.[88]

---

86 *Privacy Act 1988* (Cth) s 18N(9).

87 See, eg *F v Credit Provider* [2003] PrivCmrA 4, where a store breached s 18N by disclosing to a customer's former partner that her account with the store was in arrears.

88 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 5–18 and 5–19.

53.90 The ALRC received relatively few comments on the regulatory reach of this provision. The CCLC submitted that definition of 'report' in s 18N(9) 'is unnecessary and must be deleted unless the appropriate consumer protections are put in place and evidence is produced that this wider definition is in the public interest'.[89] In contrast, the OPC suggested that to 'promote consistency and reduce complexity',

> Part IIIA should regulate not only the uses of personal information from a credit report by credit providers but also the uses of credit worthiness information in its entirety rather than aspects of it as currently the case. This proposal also has the benefit of making the legislation clearer so that it assists businesses to understand their legal obligations and help consumers understand their rights.[90]

ALRC's view

53.91 In effect, s 18N creates a comprehensive regime with regard to the disclosure by credit providers of personal information that may have no connection with the credit reporting system. The section applies to personal information that has 'any bearing' on an individual's credit worthiness, credit standing, credit history or credit capacity. This category of information seems broad enough to include information about, for example, an individual's income, expenditure and employment and even his or her family or school connections.

53.92 The reach of s 18N is anomalous within Part IIIA, which otherwise applies only to personal information in 'credit information files' or 'credit reports' as those terms are defined in s 6(1).[91] In this context, the second reading speech indicated that the purpose of the Bill was to establish a privacy framework for the regulation of the 'consumer credit reporting industry'.

> All records of personal information held at credit reporting agencies and information from central agencies held by credit providers such as banks, credit unions, finance companies and major retailers will be covered by the new legislation.[92]

53.93 There was no reference to the establishment of a regime regulating the disclosure of all credit worthiness information held by credit providers. This resulted from the insertion of an extended definition of 'report' following amendments to the Bill proposed by the Government in 1990.

53.94 Arguably, the extended reach of s 18N can be understood as eventuating because Part IIIA was enacted before the NPPs. Section 18N was needed to ensure there was no way to avoid the application of the new credit reporting provisions by, for example, disclosure between credit providers directly, without the intermediary of a credit reporting agency. This rationale no longer applies.

---

89 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

90 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

91 With the exception of *Privacy Act 1988* (Cth) s 18Q, which applies to information obtained from credit providers by certain persons.

92 Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4216 (G Richardson).

53.95 The ALRC is not aware of any other jurisdiction that regulates personal information relating to credit worthiness in this way. In New Zealand, for example, the *Credit Reporting Privacy Code 2004* (NZ) regulates the use and disclosure of 'credit information' by the 'credit reporters' and the definition of credit information is limited to the information that credit reporters are permitted to collect.

53.96 While credit providers are well used to considering compliance with the rules for disclosing personal information in credit reporting contexts, the scope of s 18N may not be well-known (or observed) by financial institutions and other credit providers, especially non-traditional lenders. In particular, while s 18N(1)(b) permits disclosure of information relating to credit worthiness to another credit provider for a particular purposes with the specific agreement of the individual concerned, there is no general consent exception.

53.97 While the ALRC is interested in further comment on the purposes served by s 18N, there are strong arguments that the handling of personal information relating to credit worthiness should be regulated by general privacy principles and not by the *Privacy (Credit Reporting Information) Regulations*.

53.98 In Chapter 50, the ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should apply to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness (see Proposal 50–5). Consistently, there should be no equivalent in the *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*.

Proposal 53–4 There should be no equivalent in the proposed *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information related to credit worthiness. The use and disclosure limitations should apply only to personal information maintained by credit reporting agencies and used in credit reporting.

Consent and credit reporting

53.99 While the credit reporting provisions of the *Privacy Act* do not generally require the agreement of individuals to the use or disclosure of credit reporting information about them provided notification has been given, consent is required in some contexts, which are discussed below.

Consent to disclosure of information

53.100 Part IIIA contains provisions that require the agreement of an individual to the disclosure of his or her personal information. Under s 18K, an individual's agreement, sometimes in writing, is required in relation to the disclosure by a credit reporting agency of information contained in a credit report to a:

- credit provider for the purpose of assessing an application for commercial credit;[93]
- credit provider for the purpose of assessing whether to accept an individual as a guarantor;[94]
- trade insurer for the purpose of assessing insurance risks in relation to commercial credit;[95] and
- credit provider for the purpose of collecting payments overdue in respect of commercial credit.[96]

53.101 Section 18L(4) requires an individual specifically to have agreed to a credit provider using information concerning commercial credit in assessing an application for consumer credit. Finally, under s 18N, an individual must have 'specifically agreed' to the disclosure of a credit report or other credit-worthiness information by a credit provider to another credit provider for the particular purpose;[97] to a guarantor for a loan given by the credit provider to the individual concerned;[98] and to a person considering whether to offer to act as a guarantor.[99]

Disclosure to a credit reporting agency

53.102 Part IIIA does not require that an individual consent to disclosure of information by a credit provider to a credit reporting agency.[100] An individual's consent may be required, however, by the NPPs or by common law duties of confidence owed by some credit providers to their customers.

---

93 *Privacy Act 1988* (Cth) s 18K(1)(b).
94 Ibid s 18K(1)(c).
95 Ibid s 18K(1)(e).
96 Ibid s 18K(1)(h).
97 Ibid s 18N(1)(b).
98 Ibid s 18N(1)(bg).
99 Ibid s 18N(1)(bh).
100 A credit provider must not, however, give personal information to a credit reporting agency unless the individual concerned has been informed that the information might be disclosed to a credit reporting agency: Ibid s 18E(8).

53.103 Consent to disclosure may be required—at least where the credit provider is a bank[101]—to avoid breaching the duty of confidence owed by banks to their customers. This common law duty was defined in *Tournier v National Provincial and Union Bank of England*.[102] This duty is reflected in the Australian Bankers' Association's *Code of Banking Practice*, which provides that, in addition to a bank's duties under legislation, it has a general duty of confidentiality towards a customer except in the following circumstances: where disclosure is compelled by law; where there is a duty to the public to disclose; where the interests of the bank require disclosure; or where disclosure is made with the express or implied consent of the customer.[103]

'Bundled' and 'true' consent in credit reporting

53.104 Chapter 16 discusses the role of consent in privacy regulation generally. As noted in Chapter 16, problems arise where an individual's capacity to give true consent is hampered. This issue is seen most commonly in the context of 'bundled consent'—the practice of bundling together consent to a wide range of uses and disclosures of personal information without giving individuals the option of selecting which uses and disclosures they agree to.

53.105 In IP 32, the ALRC noted concerns over the use of bundled consent whereby consent to disclose personal information to a credit reporting agency is 'bundled' into a group of other consents in credit or loan applications.[104] For credit reporting agencies and credit providers, the consents may include those required under the credit reporting provisions and the NPPs. The ALRC asked what issues are raised by the practice of credit providers seeking 'bundled consent' to a number of uses and disclosures of personal information, including in relation to credit reporting.[105]

53.106 The practice of bundled consent in the context of credit reporting was criticised in a number of submissions.[106] For example, the BFSO stated:

> We do not think that consumers can be made properly aware of their rights if consent for these purposes is bundled together with other consents. In our view, all privacy

---

101 The duty may also apply to building societies, credit unions and other authorised deposit-taking institutions: A Tyree, 'Does Tournier Apply to Building Societies?' (1995) 6 *Journal of Banking and Finance Law and Practice* 206.

102 *Tournier v National Provincial & Union Bank of England* [1924] 1 KB 461. The duty extends to disclosure to related bodies corporate: *Bank of Tokyo Ltd v Karoon* [1987] AC 45, 53–54.

103 Australian Bankers Association, *Code of Banking Practice* (1993), [12.1].

104 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006); Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

105 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–14.

106 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

> notifications should be clear and separate from other contractual provisions and consent for privacy purposes should not be bundled with consent for other purposes.[107]

53.107 The Australian Privacy Foundation submitted that, in credit reporting, it is particularly important that consent for secondary purposes such as marketing be clearly separated from any notification of, or consent in relation to, disclosures involved in credit risk assessment.[108] Similarly, Legal Aid Queensland noted that, in credit reporting, 'unless consents are unbundled and not impliedly linked to the provision of services, consents do not provide adequate protection for the security of a person's financial information'.[109] The CCLC submitted that the law should be clarified to ensure that

> consumers are required to consent to the credit provider accessing their credit information from a credit reporting agency and to reporting information to a credit reporting agency, including derogatory information, at the time of applying for credit, even if such consent may be a condition of securing credit. Such consents, however, should be clearly delineated into 'consents which are necessary for you to get this loan' and consents that are optional ('you may elect not to sign/consent to any of the following').[110]

53.108 Submissions from industry emphasised that bundled consent is a practical necessity in the current regulatory environment.[111] For example, the Mortgage and Finance Association of Australia (MFAA) considered that bundled consent is the 'only practical and efficient type of consent' and is needed to 'allow the financial markets to work efficiently'.

53.109 The MFAA agreed, nevertheless, that disclosure statement can be 'unreadable', but suggested that 'the creation of safe harbour provisions and a wide pro forma general consent will overcome these problems'.[112] American Express also commented on the 'longwinded' and 'cumbersome' language required on consent forms.[113]

Consent and notification

53.110 Leaving aside issues about the nature of consent and the context in which it is obtained, there are questions about whether reliance on the principle of consent to

---

107 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

108 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

109 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

110 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 5. MasterCard also supported the imposition of such a consent requirement: MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

111 Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Optus, *Submission PR 258,* 16 March 2007.

112 Mortgage and Finance Association of Australia, *Submission PR 231,* 9 March 2007.

113 American Express, *Submission PR 257,* 16 March 2007. See also, Australian Finance Conference, *Submission PR 294,* 18 May 2007.

protect the privacy of personal information in credit reporting is effective or whether alternative approaches are preferable.[114]

53.111 It was noted in submissions that, in view of the relative bargaining positions of the parties, consent obtained in a credit application process is not 'true' consent.[115] The Australian Privacy Foundation and Waters suggested that the requirements for agreement in ss 18K and 18L should be replaced with requirements for notice.

> This would acknowledge the reality that all credit providers routinely make 'agreement' to disclose a condition of loan applications. It is not therefore free and informed consent in that individuals cannot in practice proceed with an application for credit without giving their agreement to disclosure. In these circumstances it is more 'honest' and accurate to impose only an obligation to notify – as has already been done [under s 18E(8)(c)].[116]

53.112 The Consumer Action Law Centre commented that consent requirements are largely ineffective, as terms providing that the consumer consents to the disclosure of personal information for credit reporting purposes are 'included as a matter of course in standard-form credit applications'. The Centre stated:

> For this reason, the more effective way to protect consumers from inappropriate conduct is to regulate the notification of disclosure of, and the use of, personal information.[117]

ALRC's view

53.113 Concerns about the ability of individuals to make an informed and free choice about the use or disclosure of personal information have particular relevance in credit reporting. Consent, in this context, is often a condition of assessing or granting a credit application. Access to credit, whether for a housing mortgage or mobile telephone plan, is a matter of great importance to individuals and there may be significant consequences for individuals if credit is not available.

53.114 In Chapter 16, the ALRC proposes that the OPC should provide further guidance as to how an individual's consent under the *Privacy Act* may be obtained, including in credit reporting and other financial contexts.[118] This proposal responds to a need for greater clarity as to the meaning of 'consent'.

---

114 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–15.

115 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

116 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; See also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

117 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

118 Proposal 16–1.

53.115 At present, no consent is required for the collection of credit reporting information. The ALRC considers that this position should continue under the *Privacy (Credit Reporting Information) Regulations*. However, as discussed in Chapter 52, the *Privacy (Credit Reporting Information) Regulations* should provide new notification requirements.

53.116 In drafting the *Privacy (Credit Reporting Information) Regulations*, the existing provisions requiring the agreement of the individual to specific use or disclosure should be reviewed to determine whether a notification, rather than a consent, requirement may be more appropriate where true consent is not able to be given.

53.117 It should be noted, however, that some of the existing provisions apply in circumstances where consent is more appropriate than notification, particularly where consent may be requested after credit has been granted. For example, the individual concerned may have a genuine choice about whether the disclosure will be made where asked to consent to a disclosure to another credit provider,[119] or to a guarantor or prospective guarantor.[120]

119 *Privacy Act 1988* (Cth) s 18N(1)(b).
120 Ibid s 18N(1)(bg)-(bh).

54. Data Quality and Security

Contents

Introduction 1503
Data quality 1504
Default reporting—timing and calculation 1505
Multiple listing 1507
Statute barred debts 1509
Schemes of arrangement 1511
Improving data quality 1513
Auditing credit reporting information 1513
Other means of improving data quality 1516
Data quality obligations of credit reporting agencies 1517
ALRC's view 1519
Regulating data quality 1520
ALRC's view 1520
Deletion of credit reporting information 1523
ALRC's view 1524
Data security 1526
ALRC's view 1526

Introduction

54.1 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act* dealing with the data quality and security of credit reporting information and makes proposals on how these matters should be dealt with under the proposed Unified Privacy Principles (UPPs)[1] and the proposed *Privacy (Credit Reporting Information) Regulations*.

54.2 The quality of information in credit information files is of fundamental importance to individuals, given the significant consequences that may flow, in terms of future access to credit, from an adverse credit report. Data quality, in the context of credit reporting, has a number of important aspects.

1 See Part D.

- Credit reporting information may be inaccurate because the individual has been misidentified (that is, cases of mistaken identity); or information may be 'about' the correct individual, but inaccurate for other reasons.

- Credit reporting information may be accurate in objective terms, but not comply with regulatory standards relating to data quality, such as those prescribing the permitted content of credit information files.[2]

- The consistency of data reported by credit providers is an important aspect of data quality because if the same information is reported inconsistently, it may be misinterpreted more easily.

- Overdue payment information may be considered inaccurate because the debt to which the payment relates is disputed; because information relating to the same debt has been reported multiple times; or the debt has been paid but repayment has not been recorded.

54.3 In the Issues Paper *Review of Privacy—Credit Reporting Provisions* (IP 32), the ALRC noted that consumer groups and regulators have identified ongoing problems with the quality of credit information files and credit reports.[3] Submissions in response to IP 32 provided further perspectives on the extent and nature of data quality problems in the credit reporting system. These submissions are referred in the discussion below, which highlights a number of specific issues concerning data quality before discussing means to ensure and improve data quality more generally.

54.4 Where specific concerns about data quality are serious and well-defined, and the solution is reasonably clear, it may be appropriate to deal with them through specific provisions of the *Privacy (Credit Reporting Information) Regulations*. In other cases, matters may be dealt with more effectively through detailed data quality requirements in the proposed credit reporting industry code,[4] subject to the overriding obligation to ensure that credit reporting information is accurate, up-to-date, complete and not misleading.

Data quality

54.5 The proposed 'Data Quality' principle in the UPPs provides that:

> An agency or organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the UPPs, accurate, complete, up-to-date and relevant.

---

2 *Privacy Act 1988* (Cth) s 18E.

3 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.48]–[5.52].

4 Proposal 50–11.

54.6 In Part IIIA, s 18G(a) provides that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that personal information in a credit information file or credit report is 'accurate, up-to-date, complete and not misleading'.

54.7 In addition, the *Credit Reporting Code of Conduct* provides for the steps to be taken by a credit reporting agency when it becomes aware that information supplied by a credit provider may be inaccurate. If the agency believes that other credit information files may contain similar inaccurate listings it must, as soon as practicable, notify the credit provider and request the credit provider to investigate the accuracy of other files that may be similarly affected.[5]

Default reporting—timing and calculation

54.8 Section 18E(1)(b)(vi) permits the inclusion in credit information files of information about credit where the individual is at least 60 days overdue in making a payment and the credit provider has taken steps towards recovery of the amount outstanding. There is no maximum period of time before which an overdue payment must be listed.[6]

54.9 The default reporting practices of credit providers vary considerably.[7] Submissions emphasised the need for more consistency in relation to the timing of default reporting; and in calculating the amount of the debt reported. For example, the Consumer Credit Legal Centre (NSW) Inc (CCLC) expressed concern that credit providers may list overdue payments or other debts 'a few months, weeks or even days' before they become statute barred.

> The effect of this is to extend the adverse consequences of the default nearly five (or seven in the case of a listing for a 'serious credit infringement') years beyond the limitation period. This is inconsistent with the policy prohibiting the listing of statute barred debts and should not be allowed.[8]

54.10 Several submissions suggested that regulation should provide for a maximum period of time before which an overdue payment must be listed.[9] In this context, the Telecommunications Industry Ombudsman (TIO) noted that, in its experience, there can be a significant delay (of three years or more in some cases) between a payment

---

5 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [1.4].

6 Subject to *Privacy Act 1988* (Cth) s 18E(1)(ba) (dealing with statute barred debts and guarantors); s 18F (deletion of information from credit information files).

7 See also, the discussion of compulsory reporting in Ch 52.

8 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

9 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 12; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

falling due and a telecommunications provider reporting the default to a credit reporting agency.[10]

54.11 The Consumer Action Law Centre, CCLC and Legal Aid Queensland all recommended that regulation provide that defaults must be listed within 12 months.[11] Legal Aid Queensland stated that one benefit of such a limitation was that this 'would prevent a debt collector taking assignment of a debt relisting the debt'.[12]

54.12 Submissions also commented on uncertainty about the amount of debt that should be reported. As AAPT explained:

> The issue of the 'oldest debt rule' is unclear. To give an example, if a customer currently owed us $30, and $50 was owing over 30 days, and $200 was owing over 60 days, once the 60 days passed, it is our understanding that only the $200 debt can be listed. Some suppliers consider that the entire debt owing at that 60 day point can be listed, and this is an issue that we would like to see addressed in the legislation.[13]

54.13 The position is complicated by the fact that some credit contracts have acceleration clauses. An acceleration clause is a term of a contract providing that on the occurrence or non-occurrence of a particular event (such as an overdue payment), the credit provider becomes entitled to immediate payment of all, or a part of, an amount under the contract that would not otherwise have been immediately payable.[14]

54.14 The OPC confirmed its view that, under s 18E(1)(b)(vi), 'the aggregate components of the listed amount must all be 60 days overdue'. The OPC suggested, nevertheless, that this provision may 'need to be re-drafted to make this position clearer'.[15] The BFSO also submitted that credit reporting regulation should provide clearly that the total amount of debt reported must be 60 days overdue at the time the listing is made.[16]

54.15 Legal Aid Queensland noted that the requirement for overdue payments to be more than 60 days overdue before listing has 'created problems for consumers who question why the amount shown on their credit report is different to that demanded by the creditor'.

> We would support changes so that if a person is 60 days in arrears on a payment and the whole of the debt is capable of being called up, then the totality of the debt should be listed rather than a further overdue payment. This would more accurately reflect

---

10 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

11 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 12.

12 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

13 AAPT Ltd, *Submission PR 260,* 20 March 2007.

14 *Consumer Credit Code* s 84.

15 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

16 The BFSO submitted that it should be permitted to add further arrears accrued since a default notice to the total debt reported: Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

> the totality of the position of the borrower and mean that the borrower is less confused about the status of his obligations to the lender.[17]

ALRC's view

54.16 The ALRC understands that credit providers, through the Australasian Retail Credit Association (ARCA), have been examining ways to reconcile differences between credit providers' internal accounting and reporting procedures and the default reporting allowed by the credit reporting provisions of the *Privacy Act*. ARCA's aim is to encourage credit providers to move to a consistent default reporting standard, based on reporting the full amount outstanding at the time of listing.[18]

54.17 The ALRC agrees that consistency in the timing and calculation of default reporting is a matter that should be pursued through a credit reporting industry code. It is more likely than not that an attempt to prescribe approaches to these matters by regulation would create other difficulties and ambiguities, as shown by the experience of s 18E(1)(b)(vi). Nevertheless, if industry self-regulation is not successful in addressing the existing problems, further regulation should be considered—at least with respect to some basic elements of default reporting, such as time limits and requirements to report the full amount outstanding at the time of listing.

Multiple listing

54.18 Multiple adverse listings in respect of the same debt on credit information files may occur for a range of reasons. In IP 32, the ALRC noted the following examples:[19]

- A credit provider lists an overdue payment and then makes further listings to update the amount or record another overdue payment for the same debt. This can extend the period that an overdue payment listing remains on a credit information file—potentially to the maximum term of the loan plus the five year period prescribed by s 18F(2)(c).

- A credit provider assigns a debt and the assignee automatically lists the overdue payments without checking whether the credit provider has already listed the debt; or because the assignee uses information different from that used by the original credit provider—making it difficult to determine whether the debt is the same debt.

- A credit provider lists an overdue payment and later lists a serious credit infringement with respect to the same debt. This can extend the period that an

---

17 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.
18 ARCA Default Reporting Paper October 2006.
19 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.36].

> adverse listing remains on a credit information file—potentially to five years plus the seven year period prescribed by s 18F(2)(g).

54.19 Submissions confirmed a continuing problem with multiple listings.[20] For example, Legal Aid Queensland stated that:

> A common complaint by consumers is that a debt was relisted when it was sold to an assignee. Unless they have a copy of their credit report from the relevant time period, they are unable to show that the listing was made twice. [21]

54.20 The TIO noted that it is not uncommon for consumers to have multiple contacts with a telecommunications service provider in order to make repayment arrangements. This can sometimes lead to multiple default listings, extending the period of adverse listing for the same debt.[22]

54.21 Nigel Waters of the Cyberspace Law and Policy Centre UNSW submitted that there could be an obligation on assignees to take reasonable steps to check whether the original credit provider has already listed an overdue payment, and an obligation on credit providers assigning debt to inform the assignee which if any of the assigned debts have been reported to a credit reporting agency. Waters added:

> All these suggested new requirements (and some existing ones) might be facilitated by a system of identifiers for loans (as opposed to borrowers). This should be explored with the finance industry.[23]

54.22 The CCLC considered that the law should clarify that changes to amounts owing should be made by updating the original default—that is, by altering rather than adding information.[24] Waters also suggested that

> a clear distinction could be made between marginal changes in the amount owing on a single debt (often as a result of fees and charges) and a second default on the same loan … separated by a period of 'normal' repayments. It is legitimate for such second defaults … to be listed separately whereas it is in no-one's interests for a single default to be reported and recorded multiple times.[25]

54.23 The Consumer Action Law Centre stated that multiple listings should be subject to a harsher penalty than other breaches of credit reporting regulation because multiple listings are

---

20 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

21 Legal Aid Queensland, *Submission PR 292,* 11 May 2007. Legal Aid Queensland noted that restrictions on the listing of an overdue payment after 12 months would have a significant impact on this problem.

22 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

23 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

24 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 28.

25 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007. Also Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

> damaging both to the individual concerned and to the integrity of the credit reporting system, while at the same time are preventable if credit providers and [credit reporting agencies] have the appropriate systems in place to ensure accurate data regarding matters such as account names and numbers.[26]

ALRC's view

54.24 In IP 32, the ALRC noted that the credit reporting provisions do not clearly prohibit multiple listing.[27] The OPC takes the view—based on the interaction between ss 18E and 18F—that multiple listings for the same default are not permitted by Part IIIA.[28]

54.25 The OPC supported, nevertheless, the introduction of a specific provision to prohibit multiple listings in relation to the same default. The OPC also suggested that credit reporting regulation should allow a credit provider to update the amount of the default on an individual's credit information file, without an additional listing being made.[29] This idea received support in other submissions.[30] For example, Legal Aid Queensland stated:

> A credit provider should be prohibited from listing the same debt on multiple occasions. Updating details as to the amount owing and current ownership of the debt should be encouraged but it is important to advise consumers who the original creditor was for them to determine whether they had any relationship with the creditor.[31]

54.26 The multiple listing of the same debt would probably constitute a breach of the requirements that credit reporting information be 'accurate' and 'not misleading'. A separate legislative prohibition on multiple listing may, therefore, not be necessary. Again, however, if industry self-regulation is not successful in addressing the existing problems with multiple listing further regulation should be considered.

Statute barred debts

54.27 Another data quality issue concerns the listing of statute barred debts. The *Credit Reporting Code of Conduct* states that a credit provider must not give to a credit reporting agency information about an individual being overdue in making a payment

---

26 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

27 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.37].

28 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

29 Ibid.

30 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Min-it Software, *Submission PR 236,* 13 March 2007.

31 Legal Aid Queensland, *Submission PR 292,* 11 May 2007.

where recovery of the debt by the credit provider is barred by the statute of limitations.[32]

54.28 Section 18E(1)(ba)(i) prevents statute barred debts from being listed against a guarantor's credit information file. There is, however, no parallel provision applying to the credit information files of other individuals. In IP 32, the ALRC noted that this anomaly may need to be addressed.[33]

54.29 A range of comments about statute barred debts were made in submissions. Min-it Software, which provides software for the micro-lending industry, stated that:

> we have seen instances where a default could have 4 or more references relating to it but each of which extends the statute barring period. It is our opinion this is an abuse of process by the credit reporting agencies. They have allowed this situation to occur simply because the listings are recorded by increasing date … One simple way around this would be to allocate a unique number to each default.[34]

54.30 MasterCard Worldwide (MasterCard) also proposed that legislation should require credit reporting agencies to delete default listings after a period of time has elapsed since the event occurred, rather than a period since the default was reported to the agency[35] as is currently the case under s 18F(2). Other submissions agreed that credit reporting regulation should prohibit expressly the listing of statute barred debts and ensure that borrowers and guarantors are treated consistently.[36]

ALRC's view

54.31 The rationales for statutory limitation periods on the enforceability of debts have been described as follows:

> First, as time goes by, relevant evidence is likely to be lost. Second, it is oppressive, even 'cruel', to a defendant to allow an action to be brought long after the circumstances which gave rise to it have passed. Third, people should be able to arrange their affairs and utilise their resources on the basis that claims can no longer be made against them … The final rationale for limitation periods is that the public interest requires that disputes be settled as quickly as possible.[37]

---

32 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [2.8]. See also *B v Credit Provider* [2004] PrivCmrA 2 ; *Q v Credit Provider 2* [2004] PrivCrimA 16.

33 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.33].

34 Min-it Software, *Submission PR 236,* 13 March 2007. Optus stated that credit reporting agencies should 'have an end date for all default listings' but do not 'currently have this functionality in their system': Optus, *Submission PR 258,* 16 March 2007.

35 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

36 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

37 *Brisbane South Regional Health Authority v Taylor* (1996) 186 CLR 541, 553 cited in Australian Securities and Investments Commission, *Collecting Statute-Barred Debts: An ASIC Report* (2005), 6.

54.32 While making an adverse credit listing is not to be equated with taking legal action to recover a debt, both actions may have negative consequences for the individual concerned and, with the passage of time, be more difficult to contest. Allowing the listing of statute barred debts on credit information files may be inconsistent with the public policy behind statutory limitation periods. The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of statute barred debts.

Proposal 54–1 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a State or a Territory from bringing proceedings against the individual to recover the amount of the overdue payment.

Schemes of arrangement

54.33 In IP 32, the ALRC noted that there is some ambiguity about the application of credit reporting provisions where the individual enters into a new arrangement with the credit provider to repay the debt, such as by entering into a scheme of arrangement.[38] Under the *Credit Reporting Code of Conduct*, a note indicating that a scheme of arrangement has been entered into by the individual and a credit provider may only be listed where an overdue payment or serious credit infringement has previously been listed.[39]

54.34 The OPC has stated, in its credit reporting advice summaries, that where a scheme of arrangement is entered into the 'new situation is not regarded as being information about the same default as the original entry'.[40] Therefore, if payments become overdue under the new arrangement, a new default entry may be listed and remain on the individual's credit information file for a further five year period. The OPC has recommended that this advice should be reviewed.[41]

54.35 The ALRC asked for comments on whether legislation should clarify the application of Part IIIA to payments under new arrangements with respect to the same

38 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.38].
39 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [2.10].
40 Office of the Privacy Commissioner, *Credit Reporting Advice Summaries* (2001), [9.3].
41 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

debt.[42] In response, the Energy and Water Ombudsman NSW (EWON) stated that it would support legislative clarification to

> ensure that if a credit provider (such as an energy retailer) re-lists the same debt (or part of the same debt) with a credit reporting agency, that any time the debt has already been listed for is deducted from the standard five year listing period.[43]

54.36 While MasterCard submitted that the position set out by the OPC should continue,[44] other submissions agreed that listing a default under a scheme of arrangement should not commence a new five year listing period.[45] Both these approaches may be criticised. If an overdue payment under a scheme of arrangement recommences a new five year listing period, an individual may be subject to adverse credit reporting information resulting from a default first made ten (or more) years ago. On the other hand, if a new listing period is not commenced, an individual's credit reporting information may not show that the individual is in default under a scheme of arrangement because the time period for the original debt has expired.

54.37 In the ALRC's view, the preferable position is that a new listing period should commence. This is consistent with the OPC's interpretation of the existing provisions of Part IIIA. Any other position may lead to confusion about what constitutes the 'same' debt, including for example, where several debts are consolidated.

54.38 The *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt, such as by entering into a scheme of arrangement with the credit provider, an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information file for the full five year period permissible under the regulations.

54.39 For these purposes, a new credit arrangement should mean a formal written arrangement involving a substantial renegotiation of the terms of the loan. An arrangement would normally involve a significant variation of the individual's obligations with regard to one or more of the main elements of the contract such as the period of the loan, or the size and frequency of repayments.[46]

54.40 A related issue is whether regulation should permit a scheme of arrangement to be listed on an individual's credit information file without the need for a default to be listed first. It has been suggested that such a listing could be made subject to a shorter retention period than other adverse listings. The perceived advantage of such a reform

---

42 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.39].

43 Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007.

44 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

45 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

46 See Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [55E]. This would include changes to a debtor's obligations under *Consumer Credit Code* ss 66–67.

is that it would encourage credit providers to assist individual consumers to manage potential default and avoid the detrimental implications of a default listing. The CCLC noted that any such proposal would need to 'balance the prevention of over-indebtedness with the desirability of preserving consumer options to reduce their financial difficulties by refinancing on more favourable terms'.[47]

54.41 The ALRC observes that such a move would also require a change to the existing permissible content of credit reporting information under s 18E of the *Privacy Act* and to the maximum permissible periods of retention set out in s 18F. The ALRC has not received any formal submissions in favour of such a reform, and is not convinced of its benefits.

Proposal 54–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt, such as by entering into a scheme of arrangement with the credit provider, an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information file for the full five year period permissible under the regulations.

Improving data quality

54.42 A range of comments were made in submissions about ways to ensure or improve the data quality of credit reporting information; including audits of credit reporting information, and the imposition of new obligations on credit reporting agencies.

Auditing credit reporting information

54.43 The audit of credit reporting information may assist to ensure data quality. Under the Act, the Privacy Commissioner has the function of auditing credit information files and credit reports held by credit reporting agencies and credit providers.[48] As discussed in IP 32, no credit reporting audits have been conducted since 2003–04.[49] The OPC review of the private sector provisions of the *Privacy Act*

47 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 110, rec 26.

48 *Privacy Act 1988* (Cth) s 24A(1)(g).

49 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [4.20]–[4.21].

noted that the priority given by the OPC to its complaint-handling functions has diverted resources from other areas of responsibility, including auditing.[50]

54.44 In IP 32, the ALRC asked how the Privacy Commissioner's powers to audit credit information files and credit reports operate in practice, and whether these audit powers are adequate.[51] In response, the Consumer Action Law Centre advocated strongly that the Australian Government allocate more resources to the OPC to perform its auditing functions.

> In the credit reporting regulatory scheme, the OPC is both the complaints handler and the regulator. It is therefore even more important that it identify systemic issues or incidents of non-compliance with the scheme and take action where appropriate. Undertaking audits is the key way in which information about non-compliance may be obtained proactively, with complaints received the key way in which such information is obtained reactively.[52]

54.45 Other submissions also emphasised the importance of the OPC's audit function in the credit reporting context.[53] The CCLC recommended that there should be 'adequate priority and resources' given to the audit functions of the OPC. The CCLC stated that, in addition to the importance of audits in identifying systemic issues,

> many aspects of the credit reporting system are essentially invisible because the interactions between the credit reporting agencies and their subscribers consist of private commercial arrangements and processes to which consumers or their representatives are not privy. There is considerable potential for the law to be breached without giving rise to any complaint because those affected (the end consumer of credit products) may have no awareness that a particular practice is happening. There is no effective way of monitoring compliance with these provisions apart from a system of regular, robust and independent audits.[54]

54.46 As discussed in Chapter 44, the power to audit is an important tool that the OPC should be able to use for a range of compliance purposes, not limited to credit reporting contexts. At present, however, the *Privacy Act* contains no general OPC power to audit the privacy compliance of organisations. The ALRC proposes that the *Privacy Act* be amended to provide for such a broader audit power,[55] which would encompass the existing powers to audit credit information files and credit reports held by credit reporting agencies and credit providers.

---

50 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 160. While the OPC Review referred to auditing of Commonwealth government agencies specifically, diversion of resources may also have affected credit reporting audits.

51 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 4–1.

52 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

53 National Legal Aid, *Submission PR 265,* 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007) rec 55.

54 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 159.

55 Proposal 44–6.

54.47 Auditing credit reporting information in order, for example, to assess data quality, is complex and resource intensive. In practice, audit by a regulator may not be sustainable. One submission noted that given the scale of the credit reporting system 'it is unlikely that the OPC would ever have sufficient time, funding or resources to effectively carry out privacy audits'.[56] It was suggested that the solution

> is for third-parties to carry out the privacy audits on behalf of the OPC either under licence or as registered privacy auditors. This would allow the OPC to retain control of the privacy audit function while at the same time relieving it of the burden of trying to undertake such audits itself.[57]

54.48 International credit reporting agency Experian noted that, in the United Kingdom, the Information Commissioner does not have a specific right of audit of credit reporting agencies, and

> If they did it would be virtually impossible to conduct such an audit such is the complexity of the agreements and the operating systems both at lenders and credit reporting agencies.[58]

54.49 Another possibility, suggested in a number of submissions, is to place more formal obligations on credit reporting agencies to ensure the data quality of information provided by their subscribers, including through audit processes.[59] The CCLC recommended that credit reporting agencies should be 'required to bear the cost of regular, independent audits of their operations to ensure compliance with the law and data quality standards and to report the outcomes of such audits'.[60] The Australian Privacy Foundation submitted that credit reporting agencies should be required to include data quality obligations in subscriber agreements; monitor and conduct regular checks on quality; and investigate any possible breaches.[61]

54.50 Other submissions focused on self-auditing by credit providers. Legal Aid Queensland stated that self-audits would include:

- a requirement to document internal compliance mechanisms;
- internal compliance mechanisms would include manuals, training and an audit program; and

---

56 Confidential, *Submission PR 227,* 9 March 2007.

57 The costs of audit would be borne by the credit providers themselves: Ibid.

58 Experian Asia Pacific, *Submission PR 228,* 9 March 2007.

59 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 41.

60 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 41.

61 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

- an obligation to develop systems to recognize and deal with and if necessary, report systemic breaches of the Act and any ancillary Code.[62]

54.51 The OPC stated that it supported the continuation of the Privacy Commissioner's power to conduct audits of credit reporting activities but also recommended 'the promotion of self-auditing for credit reporting compliance within the credit reporting industry'.[63]

Other means of improving data quality

54.52 A range of comments were made about other means to improve the data quality of credit reporting information. ARCA and Veda Advantage referred to the proposed implementation by credit providers and credit reporting agencies of new industry credit reporting software standards.[64]

54.53 Another observation was that a more comprehensive credit reporting system would help to improve data quality.[65] For example, MasterCard stated:

> Overseas evidence suggested that inaccuracies are 'washed out' by the more regular update of an individual's record. Indeed we understand that the vast bulk of credit record errors relate to the consumer's name (such as spelling) and address. With the implementation of more sophisticated screening software (as will be required to support comprehensive credit reporting), and greater competition in the credit reporting industry … such errors will be drastically reduced.[66]

54.54 Veda Advantage noted that increased 'consumer engagement' with their credit reports under more comprehensive reporting would enhance data quality.[67] GE Capital Finance Australasia Pty Ltd (GE Money) referred to improvements in data accuracy resulting from wider use of fully automated reporting systems. GE Money stated that increased transparency to consumers and improved data quality are 'likely to decrease disputed "negative" entries on credit files'.[68]

54.55 Credit reporting agencies and credit providers referred to the benefit, in terms of maintaining the accuracy of credit reporting information, of access to personal information in databases maintained by governments.[69] Submissions referred, for

---

62 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007.

63 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

64 Veda Advantage, *Submission PR 272,* 29 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

65 Veda Advantage, *Submission PR 272,* 29 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

66 MasterCard Worldwide, *Submission PR 237,* 13 March 2007.

67 Veda Advantage, *Submission PR 272,* 29 March 2007.

68 GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007.

69 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007; Veda Advantage, *Submission PR 272,* 29 March 2007; Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007; AAPT Ltd, *Submission PR 260,* 20 March 2007; EnergyAustralia, *Submission PR 229,* 9 March 2007; Veda Advantage, *Submission PR 163,* 31 January 2007.

example, to the value in collecting, and matching, personal information from drivers' licence databases; registers of births, deaths and marriages; and electoral rolls.[70]

54.56 A related issue concerns the linking of credit information files. Credit reporting information may be inaccurate because the individual has been misidentified and credit reporting agencies may seek to avoid misidentification by linking files. For example, Veda Advantage stated that, where an individual 'uses two or more sets of identity details to obtain credit, we will hold a file for each identity and link them via a cross reference segment'. Veda observed:

> Although there are many legitimate reasons for an individual to change their identity details, analysis shows that the presence of a cross reference is associated with a 37% higher probability that one or both files will contain derogatory data.[71]

54.57 In practical terms, the linking of files means that when an affected individual makes a credit application and the credit provider makes an inquiry, all the linked files can be accessed.[72] The OPC suggested that the ALRC consider whether there should be provisions to regulate the linking of credit information files.[73]

54.58 The OPC has expressed concern that individuals may not be notified when their credit information file has been linked, and are unlikely to become aware of the linkage unless they are refused credit.

> The Office has received several complaints about this issue. The practice of linking files in this way appears to be a gap in the privacy protections in Part IIIA. The Office also understands that credit reporting agencies may link personal information in credit files based on information supplied by third parties. However, these third-parties do not appear to have any obligations under Part IIIA of the *Privacy Act* to ensure the accuracy of the information that they supply to a credit reporting agency.[74]

Data quality obligations of credit reporting agencies

54.59 In IP 32, the ALRC noted suggestions that further obligations should be placed on credit reporting agencies to ensure the data quality of credit reporting information,[75] including that supplied to them by credit providers. The ALRC also noted that the New Zealand *Credit Reporting Privacy Code 2004* (the NZ Code) provided one model for

---

70 The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information (see Proposal 52–6). The disclosure of personal information from particular sources for credit reporting purposes should, however, continue to be regulated by the general provisions of the *Privacy Act* (and the proposed UPPs) or by state and territory privacy or other legislation, such as that dealing with registries of birth, deaths and marriages.

71 Veda Advantage, *Submission PR 272,* 29 March 2007.

72 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

73 Ibid.

74 Ibid.

75 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.55].

the imposition of such obligations.[76] Under the NZ Code, as part of a data quality rule applying to credit reporting agency, agencies must:

> (b) establish and maintain controls to ensure that, as far as reasonably practicable, only information that is accurate, up to date, complete, relevant, and not misleading is used or disclosed;
>
> (c) monitor information quality and conduct regular checks on compliance with the agreements and controls;
>
> (d) identify and investigate possible breaches of the agreements and controls;
>
> (e) take prompt and effective action in respect of any breaches that are identified; and
>
> (f) systematically review the effectiveness of the agreements and controls and promptly remedy any deficiencies.[77]

54.60 The Australian Privacy Foundation said that it agreed with the analysis of consumer groups that 'there are too few incentives, and too few sanctions to ensure compliance with the data quality obligations', and submitted that the imposition of obligations similar to those in the NZ Code is desirable.[78]

54.61 The OPC recommended the introduction of new obligations on credit reporting agencies to take reasonable and proactive steps to maintain the accuracy of credit reporting information. The OPC suggested that these provisions could be modelled on those that currently exist in the NZ Code. The OPC also suggested that it produce guidance for credit providers and credit reporting agencies about what measures are considered to be 'reasonable steps' to promote and maintain the accuracy of credit reporting information.[79]

54.62 The CCLC stated that the law should clearly define the responsibilities of credit reporting agencies, including in relation to data quality control.[80] The CCLC recommended, more generally, that 'all subscribers to the credit reporting system should be required to subscribe to a Code of Practice which addresses hardship policies and procedures in broad terms, is subject to monitoring and compliance mechanisms, and is taken into account in the decisions of an approved EDR Scheme'.[81]

54.63 In contrast, other submissions suggested that the existing obligations with regard to data quality are sufficient. EnergyAustralia stated that it 'is hard to see how further regulation could ensure greater accuracy on the part of credit providers', especially 'without a unique identifier or a database against which details can be cross-

---

76 The NZ Code requires credit reporting agencies to enter into subscriber agreements that comply with the provisions of a schedule to the Code: *Credit Reporting Privacy Code 2004* (NZ), r 8(3)(a), sch 3.

77 Ibid, r 8(3).

78 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

79 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

80 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 124.

81 Ibid, rec 25.

checked'.[82] Dun and Bradstreet also stated that current regulation concerning the accuracy of credit information files is sufficient.[83]

ALRC's view

54.64 Much of the information contained in credit information files, and provided by agencies to their subscribers in credit reports, is reported to the agencies by credit providers. Credit reporting can be described, to some extent, as operating on an 'honour system'—in that credit reporting agencies do not check the accuracy of the information given to them by credit providers.[84]

54.65 Consumer groups have expressed concerns that there is no adequate incentive for credit reporting agencies or credit providers to correct systemic flaws in the credit reporting, in part because the cost of dealing with a small number of complaints is less than the cost of ensuring the data is accurate in the first place.[85]

54.66 The ALRC considers that it is important that credit reporting agencies take more responsibility for the ensuring the data quality. This imperative is recognised by agencies themselves. Veda Advantage stated, for example, that a statutory obligation on the credit reporting agencies to be satisfied that credit providers are able to comply with data quality obligations would 'help ensure regulatory objectives are met'.[86]

54.67 The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* impose obligations on credit reporting agencies to monitor the data quality of information provided to them by credit providers, including through audits. The ALRC considers that a provision containing similar obligations to those contained in the NZ Code should be included in the *Privacy (Credit Reporting Information) Regulations*, to encourage the development of audit and other processes to ensure data quality.

Proposal 54–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure data quality in the information credit providers provide to credit reporting agencies;

82 EnergyAustralia, *Submission PR 229,* 9 March 2007.
83 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.
84 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.53].
85 See, eg, Ibid; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 135.
86 Veda Advantage, *Submission PR 272,* 29 March 2007.

(b) establish and maintain controls to ensure that only information that is accurate, complete, up-to-date and relevant is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

Regulating data quality

54.68 As noted above, the data quality obligation in Part IIIA[87] and the proposed 'Data Quality' principle are similar. It may be argued that the proposed 'Data Quality' principle is adequate to cover credit reporting information without the need for separate provisions in the *Privacy (Credit Reporting Information) Regulations*.

54.69 Although these requirements are broadly similar, there remain some important distinctions. While s 18G(a) provides an additional requirement that personal information be 'not misleading', the 'Data Quality' principle provides an additional requirement that personal information be 'relevant'. The reasons for the formulation preferred in the UPPs are set out in Chapter 24. Whether this formulation is appropriate in the context of credit reporting information is another question.

54.70 Another issue is that s 18G requires credit reporting agencies to 'take reasonable steps' to ensure the accuracy of information. It may be suggested that, given the high volume of information handled by credit reporting agencies this may 'beg the question of what they may "reasonably" do'[88]—and whether more detailed obligations are required.

ALRC's view

54.71 The ALRC considers that the existing formulation of the data quality obligation set out in s 18G(a) should be retained in the *Privacy (Credit Reporting Information) Regulations*. In particular, the requirement that credit reporting information be 'not misleading' is significant. For general privacy protection purposes such a requirement may be too ill-defined and produce unnecessary dispute. In the credit reporting context, however, information may be 'accurate' but misleading in relation to the credit worthiness of an individual. This may be, for example, due to circumstances surrounding a default listing, such as a billing failure on the part of the credit provider. Further, the relevance requirement contained in the proposed 'Data Quality' principle

87 *Privacy Act 1988* (Cth) s 18G(a).

88 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

is unnecessary as the *Privacy (Credit Reporting Information) Regulations* will continue to prescribe the permissible content of credit reporting information.

54.72 There is consensus between industry and consumer groups about the importance of ensuring quality of credit reporting information. As stated by Abacus–Australian Mutuals, ensuring data quality is 'one of the biggest challenges for all users—consumers and business alike—of the credit reporting systems'.[89] The CCLC noted:

> Inaccuracies disadvantage consumers because they create the potential to be unfairly denied credit and pursued for debts that do not belong to them. It also disadvantages credit providers because they are less able to rely on credit report information as an accurate gauge of a person's creditworthiness and leads to inefficiencies in the credit system.[90]

54.73 There is less agreement about the extent of existing data quality problems, or what should be done to remedy them. Submissions from consumers and industry highlighted a range of problems with the accuracy, timeliness and completeness of credit reporting information. On the other hand, some degree of data inaccuracy may be expected in a high-volume and complex information processing environment such as credit reporting. Veda Advantage submitted:

> Despite the anecdotal evidence to the contrary, independent research demonstrates that the data quality is very high given the highly transactional nature of the data base with over 80,000 real time transactions a day.[91]

54.74 Determining whether particular credit reporting information is 'accurate, up-to-date, complete and not misleading' is not always a simple matter. For example, where a debt is disputed, the 'accuracy' of the information may be dependent on a determination of the legal rights of the parties. Information may be 'accurate' in terms of reflecting, for example, the amount owed by an individual at the time a credit report is issued, but not comply with data quality standards because the individual is not 60 days overdue, as required by the legislation.[92]

54.75 The concept of completeness is also problematic, for example, in relation to the timing of default reporting. There is a tension, in this context, between the use of credit reporting in credit risk assessment and debt management (and debt collection). At the risk assessment 'front-end', the concern of credit providers is that the credit report provides up-to-date and complete information relevant to the credit worthiness of the individual to whom it relates. Once an individual has gone into arrears, however, a

---

89 Abacus–Australian Mutuals, *Submission PR 278,* 10 April 2007.

90 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 123.

91 Veda stated that a 2006 pilot study of 400 consumers who had recently obtained a copy of their credit information file showed: 95% of the credit file segments were entirely accurate; 4% contained a minor error, such as incorrect spelling of personal details; and 1% reported a major error with their file, such as an incorrect credit inquiry or default report listing: Veda Advantage, *Submission PR 272,* 29 March 2007.

92 *Privacy Act 1988* (Cth) s 18(1)(vi)(A).

credit provider's decision on whether to list the default may be subject to other considerations—including how best to encourage repayment or to manage overcommitment (for example, through a scheme of arrangement).

54.76 Privacy principles should ensure that credit reporting agencies and credit providers are obliged to take reasonable steps to ensure the data quality of credit reporting information. The complexity of data quality issues in credit reporting means that more prescriptive regulation is generally undesirable. Prescriptive requirements may unnecessarily increase the cost of compliance with the *Privacy Act* and transaction costs in the finance industry generally, without any significant benefit in terms of data quality.

54.77 Rather, with some exceptions—as in the case of the listing of statute barred debts—it is considered more appropriate to leave detailed data quality requirements to be dealt with in the proposed credit reporting industry code, developed with input from consumer groups and regulators. If the proposed review indicates that industry self-regulation is not successful in addressing data quality problems such as those discussed in this chapter, however, further regulation should be considered.

Proposal 54–4 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that credit reporting information is accurate, up-to-date, complete and not misleading.

Proposal 54–5 The credit reporting industry code (see Proposal 50–11) should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers. These procedures should deal with matters including:

(a) the timeliness of the reporting of personal information, such as overdue payments;

(b) the calculation of overdue payments for credit reporting purposes;

(c) obligations to prevent the multiple listing of the same debt;

(d) the updating of personal information reported, including where schemes of arrangement have been entered into; and

(e) the linking of credit reporting information where it is unclear whether the information relates to more than one individual with similar identifying details or to one individual who has used different identifying details.

Proposal 54–6 The proposed review of the *Privacy (Credit Reporting Information) Regulations* after five years' of operation (Proposal 51–3) also should consider whether further regulation is required to ensure the data quality of credit reporting information.

Deletion of credit reporting information

54.78 The proposed 'Data Security' principle provides that an agency or organisation must take reasonable steps to 'destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs'. Part IIIA of the *Privacy Act*, in contrast, contains detailed provisions requiring credit reporting agencies to ensure that personal information contained in credit information files is deleted after the expiry of maximum permissible periods set out in s 18F.[93] For example:

- information about overdue payments must be deleted five years after the day on which the credit reporting agency was informed of the overdue payment concerned;[94]
- information that, in a credit provider's opinion, an individual has committed a specific serious credit infringement must be deleted seven years after the information was included in the credit information file;[95] and
- a record of a bankruptcy order must be deleted seven years after the order was made.[96]

54.79 In IP 32, the ALRC asked how the deletion of personal information in credit information files should be regulated.[97] In response, the Australian Privacy Foundation submitted that new credit reporting regulation should 'provide for, and in some cases mandate, earlier removal of default listings for smaller debts and in a range of other "mitigating" circumstances'.[98]

54.80 More generally, the Australian Privacy Foundation and Nigel Waters favoured a 'finer-grained' credit reporting regime, with differential collection and access rules.

---

93 These periods are summarised in Ch 49.
94 *Privacy Act 1988* (Cth) s 18F(2)(c).
95 Ibid s 18F(2)(g). The definition of 'serious credit infringement' is discussed in Ch 52.
96 Ibid s 18F(2)(f).
97 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–4.
98 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

This regime, it was said, needs to be accompanied by a 'more graduated' set of retention periods.[99]

54.81 The OPC made a range of suggestions for more graduated retention periods, linked to the monetary amount of default listings.

> The provisions do not differentiate between adverse listings for minor sums and large sums. This means that in some cases even if the monetary amount in question is quite small the consequences for the individual in attracting an adverse credit listing could be serious as such a listing will persist for five or seven years.[100]

54.82 The OPC suggested that the listing period for defaults be reduced from five and seven years to periods of two and four years, respectively, for minor monetary amounts. The OPC also submitted that the ALRC consider shorter credit listing timeframes for minors.[101]

54.83 The CCLC recommended that, if telecommunications services providers are to retain access to the credit reporting system, default listings for non-credit services such as telecommunications should be removed after two years.[102]

54.84 One credit provider, ING Bank, expressed concern about the impact of the retention periods prescribed by s 18F of the *Privacy Act* on identity verification. Section 18F, it was said,

> will potentially exclude customers, who do not represent a money laundering/terrorist financing risk, from being electronically verified if they have not applied for credit in some years.[103]

ALRC's view

54.85 The retention periods prescribed by s 18F of the *Privacy Act* provide an important protection for consumers. The consequences of an adverse listing can be serious and it is important that, after some reasonable period of time, the information should be considered spent, allowing the individual to 'repair' their credit record.

54.86 It would not be appropriate, in this context, to rely on the general provisions of the 'Data Security' principle, as this would leave credit reporting agencies with too

---

99 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

100 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

101 Ibid.

102 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 15.

103 ING Bank, *Submission PR 230,* 9 March 2007. See Ch 53 on the use of credit reporting information in electronic identity verification.

much discretion. One submission noted that the regulation of retention periods is 'an area in which more rather than less prescription is desirable'.[104]

54.87 The ALRC does not consider, however, that there is any compelling case for any major change to the existing retention periods. Credit reporting information technology systems are built around these retention periods and changes may involve significant transition costs. The ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F.

54.88 One exception involves personal insolvency information. As discussed in Chapter 52, the ALRC proposes that *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth). The implementation of Proposal 52–4 would permit the collection of credit reporting information about all the types of personal insolvency administration available under the *Bankruptcy Act 1966* (Cth). These include voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act*.

54.89 The ALRC considers that information about voluntary arrangements with creditors under Part IX and Part X should be subject to a five year retention period, rather than the seven years applicable to bankruptcy.[105] An individual who has come to a voluntary arrangement with creditors should not be in a worse position than other individuals who have defaulted.

Proposal 54–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

Proposal 54–8 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of information about voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

---

104 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007. Also Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

105 Such a reform was supported by the OPC: Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

Data security

54.90 The proposed 'Data Security' principle provides that an agency or organisation must take reasonable steps to 'protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'. In Part IIIA, credit providers and credit reporting agencies have an obligation under s 18G(b) to ensure that credit information files or credit reports are 'protected, by such security safeguards as are reasonable in the circumstances, against loss, against unauthorised access, use, modification or disclosure, and against other misuse'.

54.91 In IP 32, the ALRC noted that a range of concerns about the security of credit reporting information has been identified by the OPC in the conduct of its credit reporting auditing functions.[106] The security issues included: insufficient security of the manner in which passwords and user codes were provided to new subscribers; passwords of former employees not being automatically deactivated; and the poor security of passwords in the online environment, such as the storage of passwords by web browsers.[107] In addition, it was found that some credit providers did not have provisions in their service provider contracts regarding the security and confidentiality of information, even though these contractors can obtain access to personal information held by credit providers.[108]

54.92 The ALRC asked about issues raised by regulation dealing with the security of credit information files and credit reports and how these provisions operate in practice.[109] The ALRC received relatively little comment on data security issues. Dun and Bradstreet and the Australian Finance Conference submitted that the current provisions regarding data security obligations were adequate.[110] Members of the Queensland Law Society noted that, in the light of the inadequacies identified by the OPC, there should be no move towards more comprehensive credit reporting unless 'best financial services industry security practice' is implemented.[111]

ALRC's view

54.93 The existing data security obligation in s 18G(b) provides an additional requirement, as compared to the proposed 'Data Security' principle, that personal

---

106 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.60]–[5.61].

107 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 65–66; Australian Government Attorney-General's Department, *Response to Questions on Notice for Attorney-General's Portfolio: Senate Legal and Constitutional Legislation Committee Additional Estimates 2003–2004, Questions 38 to 50*, undated, Answer to Q 42.

108 Australian Government Attorney-General's Department, *Response to Questions on Notice for Attorney-General's Portfolio: Senate Legal and Constitutional Legislation Committee Additional Estimates 2003–2004, Questions 38 to 50*, undated, Answer to Q 42.

109 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–6.

110 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Australian Finance Conference, *Submission PR 294,* 18 May 2007.

111 Queensland Law Society, *Submission PR 286,* 20 April 2007.

information be protected from 'unauthorised use'. The proposed 'Data Security' principle does, however, refer to the 'misuse' of personal information, which seems broad enough to cover unauthorised use.

54.94 The ALRC considers that the proposed 'Data Security' principle is adequate to cover credit reporting information and no separate provision dealing with data security is needed in the *Privacy (Credit Reporting Information) Regulations*.

Proposal 54–9 The proposed *Privacy (Credit Reporting Information) Regulations* should contain no equivalent to s 18G(b) and (c), dealing with the security of credit information files and credit reports, as these obligations are adequately covered by the proposed 'Data Security' principle.

55. Rights of Access, Complaint Handling and Penalties

Contents

Introduction 1529
Access and correction 1529
Access to credit reporting information 1530
Correction of credit reporting information 1535
Notification of adverse credit reports 1536
Complaint handling 1540
Complaint-handling bodies 1540
Complaint-handling processes 1543
External dispute resolution 1548
Time limits on disputed credit reporting information 1551
Penalties 1554

Introduction

55.1 This chapter discusses the existing provisions of Part IIIA of the *Privacy Act 1988* (Cth) dealing with individual rights of access to, and correction of, credit reporting information and makes proposals on how these matters should be dealt with under the proposed Unified Privacy Principles (UPPs)[1] and the *Privacy (Credit Reporting Information) Regulations*.

55.2 The chapter also examines complaint handling in credit reporting disputes by the Office of the Privacy Commissioner (OPC) and other complaint-handling mechanisms, and penalties for breach of the proposed *Privacy (Credit Reporting Information) Regulations*.

Access and correction

55.3 The proposed 'Access and Correction' principle provides that, subject to a range of exceptions:

> If an organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information …

1 See Part D.

55.4 The proposed 'Access and Correction' principle provides that if an organisation charges for providing access to personal information, those charges must not be excessive and must not apply to lodging a request for access.

55.5 In relation to correction rights, the proposed 'Access and Correction' principle provides that an organisation must take reasonable steps to correct personal information so that it is accurate, complete, up-to-date and relevant; and notify any other entities to whom the personal information has already been disclosed prior to correction, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

55.6 Part IIIA contains similar provisions relating to personal information in credit information files and credit reports. Section 18H provides that credit reporting agencies and credit providers must take reasonable steps to ensure that individuals can obtain access to their credit information files and credit reports. Credit reporting agencies and credit providers must also take reasonable steps, under s 18J, to alter files or reports to ensure files and reports are accurate, up-to-date, complete and not misleading.

55.7 There are, however, significant differences between the rights of access and correction in Part IIIA and the proposed 'Access and Correction' principle. These differences include the absence of exceptions to the rights of access in Part IIIA; and the specific provisions in Part IIIA dealing with the inclusion of statements on the request of an individual.[2] While the proposed 'Access and Correction' principle (like NPP 6.4) provides that access charges 'must not be excessive', Part IIIA is silent on charging for access.

Access to credit reporting information

55.8 All major Australian credit reporting agencies provide individuals with access to their own credit reports on request and free of charge.[3] In the year ended June 2006, 236,168 consumers obtained a copy of their credit information file from Veda Advantage.[4] In many cases, an individual requests access to his or her credit information file because he or she has been refused credit.

55.9 Veda Advantage provides access free of charge by post within 10 working days; or for $27 within one working day by email, facsimile or mail.[5] Dun and Bradstreet provides access free of charge by post within 10 working days; or for $25 posted by express mail within one working day.[6] Tasmanian Collection Service provides access

---

2 Where a credit reporting agency or credit provider does not amend personal information as requested, the individual concerned may request the credit reporting agency or credit provider to include in a statement of the correction, deletion or addition sought: *Privacy Act 1988* (Cth) s 18J(2). Under s 18J(3) a credit reporting agency or credit provider may refer a statement considered to be of undue length in the circumstances to the Privacy Commissioner for a decision on alteration of the statement.

3 Ibid s 18H does not require that access be free of charge to the individual concerned.

4 Veda Advantage, *Submission PR 272,* 29 March 2007.

5 Veda Advantage, *Discover Your Credit History* (2005) <www.mycreditfile.com.au> at 1 August 2007.

6 Dun & Bradstreet, *Your Individual Credit File* (2006) <www.dnb.com.au> at 1 August 2007.

to credit information files free of charge 'where the request relates to an individual's refusal of credit, or is otherwise related to the management of the individual's credit arrangements' and, otherwise, for $13.[7]

55.10 Some credit reporting agencies actively encourage individuals to obtain access to their own credit information files. The Veda Advantage website notes the benefits in doing so to 'ensure your information is accurate and up to date to avoid unwanted surprises when you next apply for credit'.[8] Veda also offers a service, named 'Credit Alert', that, for a fee, notifies an individual whenever someone obtains the individual's credit information file or there is an addition or change to the information included in the file.[9] It has been suggested that individuals should check their credit reports periodically to protect themselves against the consequences of credit fraud.[10]

55.11 In the Issues Paper, *Review of Privacy—Credit Reporting Provisions* (IP 32), the ALRC asked what issues are raised by the provisions of the *Privacy Act* dealing with individuals' rights of access to, and alteration of, information in credit information files and credit reports.[11]

Promoting individual access

55.12 Submissions referred to the importance of promoting individual access to credit reporting information in helping to ensure data quality and, more generally, in making the credit reporting system more transparent to consumers.[12] The Consumer Credit Legal Centre (NSW) Inc (CCLC) noted:

> As credit history information is collected by credit providers and held by credit reporting agencies, consumers are removed from any sense of ownership of the information held about them. Consumers do not have control over the type of information that is being held, they are reliant on the credit reporting agencies for access to the information, they do not control who else can have access to their information, and they do not have the authority to change and correct the information, yet the information can be used to their detriment.[13]

55.13 One way to address the absence of a 'sense of ownership' is to encourage individuals' awareness of credit reporting system and the content of credit reporting information about them. The CCLC recommended that credit reporting agencies and government, in consultation with consumer groups, should

---

7 Tasmanian Collection Service, *TCS Credit Reports* (2006) <www.tascol.com.au/reports.htm> at 1 August 2007.

8 Veda Advantage, *Discover Your Credit History* (2005) <www.mycreditfile.com.au> at 1 August 2007.

9 Veda Advantage, *My Credit Alert Information* (2006) <www.mycreditfile.com.au> at 1 August 2007.

10 Australasian Consumer Fraud Taskforce, *Scams Target You: Protect Yourself*, 31 January 2007.

11 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–8.

12 Veda Advantage, *Submission PR 272,* 29 March 2007; Westpac, *Submission PR 256,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Edentiti, *Submission PR 210,* 27 February 2007.

13 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 69.

> ensure the public is better informed about credit reporting law and practice, the need to regularly check your individual credit report, how to dispute inaccuracies, and the possible ramifications of derogatory credit information.[14]

55.14 Westpac suggested the development of an education program designed to inform consumers that they can regularly check the accuracy of their credit report.[15] Information technology company Edentiti highlighted technology that is available to permit individuals to be given 'greater, real-time access to their records' and be 'informed whenever any activity occurs in relation to their records'.[16]

55.15 Each year around 1.5% of individuals who have credit information files obtain a copy of their file.[17] Veda Advantage have indicated a desire to see this figure increase to around 10% in five years. Veda Advantage noted, however, that achieving this target may require automated processes and access to electronic identity verification using government registries.[18]

Charging for access

55.16 Some stakeholders suggested that individuals should have a legislative right to obtain a copy of their credit reporting information free of charge.[19] The Consumer Action Law Centre stated that credit reporting information is 'important personal information and every person should have free access in order to ensure it is accurate and fair' and noted that the *Credit Reporting Act 1978* (Vic) provides for a right of access to a credit report at no cost.[20]

55.17 The CCLC noted that, in the United States, 'consumers get a free credit report every 12 months so there is more of a sense of control, and people feel more responsible for their credit data'.[21] The problems of such an approach may, however, include the cost and privacy concerns involved with sending a report to an individual's last known address. The CCLC recommended that credit reporting agencies should be obliged to provide a free copy of an individual's credit report to that individual and to 'publicise prominent information about how to get a free copy of your credit report'.[22]

---

14 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 3.

15 Westpac, *Submission PR 256,* 16 March 2007.

16 Edentiti, *Submission PR 210,* 27 February 2007.

17 Veda Advantage, *Submission PR 272,* 29 March 2007.

18 Ibid.

19 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 3.

20 *Credit Reporting Act 1978* (Vic) s 4.

21 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 69.

22 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 4.

55.18 The OPC submitted that legislation should 'contain provisions regarding when individuals should be granted access to their credit information file without charge'.[23]

Purposes of access

55.19 In 1992, Professor Graham Greenleaf warned that the right of access in s 18H might be used as a 'backdoor' means of access by organisations prohibited from obtaining credit reports.

> There is nothing in the legislation to prevent an employer, insurer, State Government licensing authority or real estate agent from requesting or requiring a person to supply a copy of their file as a condition of being considered for a position, licence, etc.[24]

55.20 The National Privacy Principles (NPPs) and state privacy legislation enacted since these comments were made,[25] provide some additional protection. For example, NPP 1 of the *Privacy Act* (like the proposed 'Collection' principle of the UPPs) provides that an organisation must not collect personal information unless the information is necessary for its functions or activities.

55.21 In IP 32, the ALRC asked whether there is any evidence that employers, insurers or government agencies request individuals to provide copies of their credit reports for employment, insurance, licensing or other purposes unrelated to the provision of credit and, if so, what steps should be taken to address this issue.[26]

55.22 In response, the OPC stated that it has received complaints and inquiries from individuals about this practice. The Office suggested that consideration be given to a legislative provision prohibiting the collection of an individual's credit information file by employers, insurers and government agencies.[27]

55.23 The CCLC expressed concern that legislative limitations on the use and disclosure of credit reporting information should not be 'subject to possible circumvention by forcing the individual to access and produce their own report'. The CCLC recommended that an offence should be created under the *Privacy Act* in relation to 'requiring an individual to provide a copy of his/her credit report in the course of any business or enterprise'.[28]

---

23 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007

24 G Greenleaf, 'The Most Restrictive Credit Reference Laws in the Western World?' (1992) 66 *Australian Law Journal* 672, 674.

25 Eg, *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic).

26 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–7.

27 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

28 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 36.

55.24 Other submissions considered that there should be less restriction on individuals providing access to their credit reporting information to third parties (that is, persons other than the individual, credit reporting agency or a credit provider for credit-related purposes). Veda Advantage stated:

> Individual consumers are also hampered by Part IIIA particularly those may wish to provide access to their credit files for a wider range of purposes than currently permitted, including accessing credit or employment overseas.[29]

55.25 The Institute of Mercantile Agents referred to

> a growing trend, especially by larger employers such as multi-nationals concerned about the prospects of fraudulent behaviour and seeing the provision of credit histories as a positive identification step. Similarly, insurers may well be keen in the face of a suspicious claim say for a vehicle theft or fire damage of premises to require a claimant to produce his/her personal credit history … If there are legitimate grounds for access, especially when initiated by the individual concerned, then access ought to be granted—with the credit history information recorded, the ability to provide low cost access should be not be at all difficult or onerous.[30]

55.26 Part IIIA places some specific constraints on direct access to credit reporting information by third parties. Section 18H(3) of the *Privacy Act* states that an individual's rights of access under the section

> may also be exercised by a person (other than a credit provider, mortgage insurer or trade insurer) authorised, in writing, by the individual to exercise those rights on the individual's behalf in connection with:
>
> (a) an application, or a proposed application, by the individual for a loan; or
>
> (b) the individual having sought advice in relation to a loan.

55.27 In Chapter 62, the ALRC concludes that the *Privacy Act* does not provide adequate discretion to agencies and organisations in dealing with informal arrangements concerning decision making under the Act, including in relation to access rights. The ALRC proposes reforms to deal more flexibly with circumstances in which privacy rights may be exercised on behalf of an individual by another person. These include the development of OPC guidelines for practices and procedures that allow for the involvement of third parties to assist with privacy decisions where the individual provides consent. These guidelines may encourage, for example, processes for obtaining consent by telephone.[31]

55.28 Section 18H(3), by requiring authorisation in writing and limiting the purposes in relation to which an individual's access rights may be exercised by another person, may be seen as contrary to the more flexible policy approach taken by the ALRC. On the other hand, the privacy risks involved with credit reporting information—including,

---

29 Veda Advantage, *Submission PR 272,* 29 March 2007.
30 Institute of Mercantile Agents, *Submission PR 270,* 28 March 2007.
31 See Proposal 62–1.

for example, the risk of identity fraud—may justify the more stringent approach taken in s 18H(3).

ALRC's view

55.29 Part IIIA does not require that an individual consent to disclosure of information by a credit provider to a credit reporting agency and individuals have limited ability to control the subsequent use or disclosure of credit reporting information about them. The ALRC agrees that, in this context, individuals' access to credit reporting information about them should be promoted, including by ensuring that individuals have a right to obtain access free of charge.

55.30 The major credit reporting agencies already provide credit reports free of charge to the individuals concerned. Some concerns have been expressed about credit reporting agencies advertising fast access to reports for a fee but 'burying in the fine print the fact that you can get your credit report free of charge'.[32] In general, however, the ALRC's impression is that individuals' access to credit reports is being facilitated adequately. The ALRC is interested in further comment on whether the right to obtain a report free of charge should be included in the proposed *Privacy (Credit Reporting Information) Regulations* and, if so, in what form.

55.31 The ALRC is not convinced that there is a need for any new legislative provision prohibiting the collection of an individual's credit reporting information by third parties, such as employers, insurers or government agencies, through the individual concerned. The collection of credit reporting information for non-credit related purposes should be regulated adequately by the proposed 'Collection' principle of the UPPs and by proposed reforms in relation to the definition of 'consent' under the *Privacy Act*.

Question 55–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide that individuals have the right to obtain a free copy of their credit reporting information?

Question 55–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide an equivalent to s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised by a person authorised in writing and for a credit-related purpose?

Correction of credit reporting information

55.32 In IP 32, the ALRC noted that consumer groups have claimed that there are, in practice, no adequate procedures to ensure that inaccurate information is removed from

32 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 49.

credit information files or credit reports at the request of the individual concerned.[33] Some of these difficulties were seen as arising from the dispute settling procedures for credit reporting. Others, however, were attributed to the drafting of s 18J.

55.33 In particular, s 18J(2) provides for the inclusion of a statement on the file or report in circumstances where the credit reporting agency 'does not amend' the information in accordance with an individual's request. It was submitted that:

> This poor drafting effectively provides no incentive for the credit reporting agency to comply with the requirement of ensuring that the credit report is accurate. In practice, all that the credit reporting agency is required to do under this section is to include a statement of the amendment sought and to notify people nominated by the individual of the amendment made, if any, or the statement of the amendment sought.[34]

55.34 In response to IP 32, the Australian Privacy Foundation submitted that, for the avoidance of doubt, the law should be amended to require correction where it is determined objectively that information is inaccurate, out of date, incomplete or misleading[35] (the terms used in s 18G of the *Privacy Act*). The ALRC agrees that this drafting problem should be remedied in the equivalent provision of the proposed *Privacy (Credit Reporting Information) Regulations*, consistently with the wording of the proposed 'Access and Correction' principle.[36]

Proposal 55–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to access and correct credit reporting information based on the provisions currently set out in ss 18H and 18J of the *Privacy Act*.

Notification of adverse credit reports

55.35 Under s 18M, when an individual's application for credit is refused based wholly or partly on a credit report, the credit provider must give the individual written notice of that fact and advice about the individual's right to obtain access to his or her credit information file held by the credit reporting agency. In IP 32, the ALRC asked about the issues raised by this provision and what obligations should apply when an application for credit is refused based on a credit report.[37]

55.36 One issue raised in submissions concerns notification of credit scoring processes. If an individual is refused credit based on a credit score this fact will not be

---

33 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [5.70].

34 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

35 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

36 UPP 9.

37 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 5–17.

apparent from the credit report. Credit scoring, as described in Chapter 48, may be described as the use of 'mathematical algorithms or statistical programmes that determine the probable repayments of debts by consumers, thus assigning a score to an individual based on the information processed from a number of data sources'.[38] A range of different data items, derived from credit reporting information or from a credit provider's own records, may be used in credit scoring.

55.37 The Australian Privacy Foundation submitted that

> there should be a clear statutory right of access to credit scores and other rankings held by [credit reporting agencies] and [credit providers], together with explanatory material on scoring systems and current thresholds for acceptance, to allow individuals to better understand how they are being assessed.[39]

55.38 The Foundation noted that the right of access provided by Part IIIA applies only to information in credit information files and credit reports[40] and a credit score is not permitted content under s 18E.[41] It stated that credit reporting agencies and credit providers rely on the 'evaluative information' exception in NPP 6.2 (retained in the proposed 'Access and Correction' principle),[42] to avoid giving individuals credit scores or rankings and provide an 'explanation' instead.[43]

55.39 In the United States, the *Fair Credit Reporting Act 1970* (US) (FCRA) requires credit reporting agencies to provide prescribed information to individuals about the use of credit scoring, on request. The FCRA provides:

> (1) *In general*. Upon the request of a consumer for a credit score, a consumer reporting agency shall supply to the consumer a statement indicating that the information and credit scoring model may be different than the credit score that may be used by the lender, and a notice which shall include--
>
> (A) the current credit score of the consumer or the most recent credit score of the consumer that was previously calculated by the credit reporting agency for a purpose related to the extension of credit;
>
> (B) the range of possible credit scores under the model used;
>
> (C) all of the key factors that adversely affected the credit score of the consumer in the model used, the total number of which shall not exceed four …
>
> (D) the date on which the credit score was created; and

---

38 F Ferretti, 'Re-thinking the Regulatory Environment of Credit Reporting: Could Legislation Stem Privacy and Discrimination Concerns' (2006) 14 *Journal of Financial Regulation and Compliance* 254, 261.

39 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

40 *Privacy Act 1988* (Cth) s 18H.

41 New Zealand credit reporting regulation permits credit reporting information to include a credit score: *Credit Reporting Privacy Code 2004* (NZ) cl 5, definition of 'credit information'.

42 UPP 9.2.

43 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

> (E) the name of the person or entity that provided the credit score or credit file upon which the credit score was created.[44]

55.40 The ALRC does not consider that simply providing rights of access only to credit scores would serve any useful purpose. However, requiring the provision of explanatory material about the key factors that adversely affected the credit score of an individual where credit has been refused seems more worthwhile.

55.41 In the United States, credit reports provided to individuals include information about the factors that affect an individual's credit score adversely (or favourably). For example, a sample MyFICO score summary lists the following as negative factors:

- You have a public record and a serious delinquency on your credit report.
- You have multiple accounts showing missed payments or derogatory descriptions.
- The balances on your non-mortgage credit accounts are too high.

55.42 Factors listed as helping the credit score include:

- You have an established credit history.
- You have an established revolving credit history.
- You currently have a good number of credit accounts.[45]

55.43 The ALRC recognises that, as information relevant to some of these factors is not available from credit reporting agencies under current credit reporting regulation, different factors would apply under Australian credit scoring conditions. The ALRC proposes, nevertheless, that the proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused should include any credit score or ranking used by the credit provider, together with explanatory material on the scoring system used.

55.44 Apart from credit scoring, there may be other reasons for credit being refused that are based on credit reporting information, but not readily apparent from an individual's access to their credit report. The CCLC submitted, for example, that:

> The law should be clarified to ensure that individuals who are refused credit on the basis that their file has been cross-referenced to another file, or any other reason that is based on information held by a credit reporting agency that is not apparent from the copy of the file the individual would be given upon request, are entitled to be given adequate information to enable them to correct any inaccuracies or false assumptions attributable to the data held by the credit reporting agency. [46]

---

44 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US), § 1681g(f)(1).

45 Fair Isaac Corporation, *Sample FICO Score Summary* (2007) <www.myfico.com/Products/FICOOne/Sample/FICOScore/Sample_Summary.aspx> at 1 August 2007.

46 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 23.

55.45 Concerns about the linking of credit information files generally are discussed in Chapter 54. The ALRC proposes that the credit reporting industry code[47] should promote data quality by mandating procedures dealing with, among other matters, the linking of credit reporting information.[48]

55.46 Concerns have also been addressed about automated decision making in risk assessment more generally. For example, the Australian Privacy Foundation stated:

> We understand that fully automated assessment of loan applications is common, using highly sophisticated credit scoring systems. However predictive and accurate these systems are, and however efficient they are compared to human judgement, they cannot be 'fair' in all individual cases.[49]

55.47 National Legal Aid also expressed concern that automated decision making in risk assessment 'poses a risk that any individual listing or inquiry or pattern of listings and inquiries recorded on the credit reference database may result in an automatic refusal of credit' and that the *Privacy Act* does not provide 'adequate safeguards against the unfairness that may result'.[50] The Australian Privacy Foundation and Nigel Waters of the Cyberspace Law and Policy Centre submitted that credit providers should be required to offer applicants an opportunity for a human review of any adverse decision.[51]

55.48 The OPC suggested that the *Privacy Act* be amended to include a more general requirement that agencies and organisations have in place adequate review mechanisms for automated decisions.[52] This idea is rejected by the ALRC, for reasons set out in Chapter 7. Rather, the ALRC proposes that the OPC issue guidance on when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.[53] In the context of credit reporting specifically, while it might be desirable to provide for rights to have an automated decision reviewed under an industry code, the ALRC does not consider it necessary to establish such a right in legislation.

Proposal 55–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to be notified where a credit provider refuses an application for credit based wholly or partly on credit reporting information, based on the provisions currently set out in s 18M of the *Privacy Act*.

---

47 See Proposal 50–11.
48 Proposal 54–5.
49 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.
50 National Legal Aid, *Submission PR 265,* 23 March 2007.
51 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.
52 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.
53 Proposal 7–5.

Proposal 55–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed.

Complaint handling

55.49 The following section of this chapter examines aspects of complaint handling in relation to credit reporting. This material should be read in conjunction with Chapter 45, which deals with the investigation and resolution of privacy complaints generally. In Chapter 45, the ALRC makes a range of proposals intended to streamline and increase transparency in the resolution of privacy complaints, including in relation to credit reporting complaints. These proposals are intended, among other things, to:

- free up the Privacy Commissioner from dealing with individual complaints to enable more of a focus on systemic issues;
- give the Commissioner more discretion not to investigate complaints, including where an external dispute resolution (EDR) mechanism could handle the complaint;
- clarify the Commissioner's conciliation function in the *Privacy Act* and give complainants and respondents the power to compel a determination when conciliation has failed; and
- give the Commissioner power to remedy systemic issues, for example, by requiring an organisation, such as a credit reporting agency, to undertake prescribed action for the purpose of ensuring compliance with the proposed UPPs.

Complaint-handling bodies

55.50 Complaints about credit reporting may be handled by credit reporting agencies and credit providers, EDR schemes such as the Telecommunications Industry Ombudsman (TIO) and Banking and Financial Services Ombudsman (BFSO), or by the OPC under the *Privacy Act*.

Credit reporting agencies and credit providers

55.51 Under the *Credit Reporting Code of Conduct*, credit reporting agencies and credit providers must establish procedures to deal with disputes relating to credit

reporting.[54] Credit providers that are financial services providers under the *Corporations Act 2001* (Cth) are required to establish internal dispute resolution systems that comply with standards set by the Australian Securities and Investments Commission (ASIC).[55] Internal dispute resolution systems may also be required by industry codes, such as the *Code of Banking Practice*[56] or by the terms of membership of EDR schemes.

55.52 The *Credit Reporting Code of Conduct* makes credit reporting agencies responsible for attempting to resolve disputes between credit providers and individuals where the dispute involves the content of a credit report. The Code states:

> 3.3 A credit provider should refer to a credit reporting agency for resolution a dispute between that credit provider and an individual where the dispute concerns the contents of a credit report issued by the credit reporting agency.
>
> 3.4 In referring a dispute to a credit reporting agency, a credit provider must inform the individual of the referral and must provide the individual with the name and address of the credit reporting agency.
>
> 3.5 Upon receipt, from a credit provider, of a referral of a request for dispute resolution, a credit reporting agency must handle the request as if the request had been made directly to the agency by the individual concerned.
>
> …
>
> 3.7 Where a credit reporting agency establishes that it is unable to resolve a dispute it must immediately inform the individual concerned that it is unable to resolve the dispute and that the individual may complain to the Privacy Commissioner.[57]

55.53 After receiving a complaint about the content of a credit report, Veda Advantage recommends that the complainant first contact the credit provider responsible for the listing to resolve the issue. If that is unsuccessful, Veda conducts an investigation 'on the consumer's behalf'.[58] Veda Advantage advised that it 'completed 22,119 investigations on behalf of consumers' in the year ending June 2006.[59] Veda stated that:

> Approximately 34% of investigations require assistance from our subscribers before they can be resolved … Others involve reference to external parties such as the Insolvency and Trustee Service of Australia … 47% of complaints require minor investigation … or an internal check, usually on data quality issues …[60]

55.54 Submissions expressed some concern about the adequacy of internal dispute resolution by credit providers—and non-traditional credit providers, such as utilities and medical practices. The Consumer Action Law Centre stated:

---

54 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), Part 3.
55 *Corporations Act 2001* (Cth) s 912A(2)(a).
56 Australian Bankers Association, *Code of Banking Practice* (1993).
57 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991).
58 Veda Advantage, *Submission PR 272,* 29 March 2007.
59 Ibid.
60 Ibid.

> These businesses often do not have credit reporting dispute resolution procedures in place as interaction with the credit reporting system may not be a major part of their operations. In fact, some have no dispute resolution systems at all. This problem takes on a larger dimension when it is remembered that the OPC routinely refers consumers with a complaint back to the credit provider for resolution.[61]

55.55 The BFSO submitted that all credit providers and credit reporting agencies should be required to have 'transparent, efficient and effective' internal dispute resolution processes and suggested that the new International Standard for internal complaints handling would be an appropriate model.[62]

External dispute resolution schemes

55.56 Many credit providers are members of EDR schemes, including financial services providers who are required by the *Corporations Act* to belong to an EDR scheme approved by ASIC.[63]

55.57 ASIC approved and other EDR schemes deal with some complaints about credit reporting. The TIO, for example, receives and resolves complaints concerning credit reporting by telecommunications service providers.[64] The TIO advised that, in the six months to December 2006, it received 1,437 complaints concerning credit reporting.[65]

55.58 The BFSO resolves some complaints concerning credit reporting by banks and their affiliates.[66] The BFSO stated that in a five-year period to December 2006, it closed 517 cases where 'privacy' or 'credit reporting' was recorded as a 'problem type'.[67] The BFSO noted, however, that problems with credit reporting commonly arise in the course of disputes about other matters such as debts, and the credit reporting aspect 'is not always captured by the BFSO data collection system if the credit reporting issue is incidental to the main issues in dispute'.[68]

55.59 Other utilities and finance industry ombudsmen—such as the Energy and Water Ombudsman NSW, the Credit Ombudsman Service and the Credit Union Dispute Resolution Centre—may also deal with credit reporting complaints.

---

61 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

62 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Standards Australia, *Customer Satisfaction Guidelines for Complaints Handling in Organizations: AS ISO 10002–2006* (2006).

63 *Corporations Act 2001* (Cth) s 912A(2)(b).

64 The TIO is wholly funded by telecommunications service providers, who are required by law to be part of, and pay for, the TIO Scheme: *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 126.

65 Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

66 Banking and Financial Services Ombudsman, *Case Studies* <www.abio.org.au> at 1 August 2007. Non-bank institutions and their affiliates can also apply to join the BFSO scheme: Banking and Financial Services Ombudsman, *About Us* <www.abio.org.au> at 1 August 2007.

67 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

68 Ibid.

The Office of the Privacy Commissioner

55.60 The *Privacy Act* provides an avenue for individuals to complain to the Privacy Commissioner about an act or practice that may be an interference with their privacy.[69] The Act sets out detailed provisions on how the Commissioner can receive, investigate and resolve complaints, including credit reporting complaints.[70] The investigation and resolution of complaints under Part V of the Act is discussed in detail in Chapter 45.

55.61 The OPC submitted that, as the credit reporting provisions of the *Privacy Act* protect the personal credit information of individuals, credit reporting complaints should continue to be handled as privacy complaints under the *Privacy Act*.[71] The OPC stated that, in the five-year period from 1 January 2002 to 31 December 2006, 17% of the complaints received by the OPC[72] concerned credit reporting issues. Of these credit reporting complaints cases, 87% had been closed as at 7 February 2007.

> Of those closed cases, approximately one third were closed following conciliation or where the credit provider had already taken steps to adequately deal with the matter. Resolutions in these cases commonly included the amending of records and, on occasion, also included the payment of compensation. Another third of the cases were closed on the basis that the respondent had not breached the Act.[73]

Complaint-handling processes

55.62 In IP 32, the ALRC noted a range of criticisms that have been made about the handling of credit reporting complaints.[74] These included concerns that:

- in order to initiate a credit reporting complaint with the OPC, complainants may be required to contact the credit reporting agency to obtain a copy of their credit information file and then to complain to the credit provider;[75]

- dispute resolution procedures established by credit providers and credit reporting agencies lack transparency and fail to address complaints in relation to repeated problems or possible systemic issues;[76] and

---

69 *Privacy Act 1988* (Cth) s 36(1).

70 Ibid s 6 defines a 'credit reporting complaint' as a complaint about an act or practice that, if established, would be an interference with the privacy of the complainant because: (a) it breached the Code of Conduct; or (b) it breached a provision of Part IIIA.

71 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

72 In the year to 30 June 2006, the OPC received a total of 1,183 complaints across all areas of its jurisdiction (1,275 were received in 2004–05): Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 29.

73 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

74 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [4.28]–[4.33].

75 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 139.

76 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.11].

- dispute resolution procedures generally place the onus of proving that listings are inaccurate on individuals who lack any real negotiating power.[77]

55.63 In IP 32, the ALRC asked how the procedures under the *Privacy Act* and the *Credit Reporting Code of Conduct* for making and pursuing complaints about credit reporting operate in practice, and what other complaint-handling mechanisms would enhance compliance and the resolution of complaints.[78]

The 'complaint merry-go-round'

55.64 Submissions emphasised concerns[79] about what has been termed the credit reporting complaints 'merry-go-round'.[80] Section 41(1A) of the Act provides that the Commissioner must not investigate a complaint if the complainant did not complain to the respondent before making the complaint to the Commissioner. Consistently, the *Credit Reporting Code of Conduct* provides that:

> The Privacy Commissioner may decide not to investigate a complaint about a credit reporting dispute if the Commissioner considers that:
>
> (a) the dispute should first be dealt with by a credit reporting agency or credit provider; or
>
> (b) the dispute is being, or has been, dealt with adequately by the credit reporting agency or credit provider.[81]

55.65 Under the *Privacy Act*, the respondent to a complaint is the person who engaged in the act or practice that is the subject of the complaint.[82] In the case of credit reporting complaints, it is often unclear whether the problem has been caused by the credit provider or the credit reporting agency, making the respondent to the complaint hard to identify.[83]

55.66 The Consumer Action Law Centre observed that the most common way in which an individual discovers inaccurate information is when the individual obtains a copy of his or her credit report, usually after an application for a loan has been rejected on the basis of the credit report.

> This generally means that the consumer makes a complaint to the [credit reporting agency]. Under the Code, the [credit reporting agency] must try to resolve the dispute but, where it cannot, it is required to inform the individual concerned that it is unable

---

77 Ibid, [5.11].

78 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Questions 4–2 and 4–3.

79 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; National Credit Union Association Inc, *Submission PR 226,* 9 March 2007.

80 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; J Corker and C Bond, 'The Merry-Go-Round: Credit Report Complaint Handling under the Privacy Act' (2001) 8(5) *Privacy Law and Policy Reporter* 1.

81 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [3.17].

82 *Privacy Act 1988* (Cth) s 36(8).

83 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

> to resolve the dispute and that the individual may complain to the OPC (not to the credit provider).
>
> Unfortunately, the practice of the OPC upon receipt of these complaints is to … refer the consumer to the relevant credit provider before it will take the complaint, even though the consumer has already complained to the [credit reporting agency] (and the [credit reporting agency] would most likely have dealt with the credit provider in its investigation of the complaint). If the credit provider cannot or does not resolve the complaint, under the Code they must refer it back to the [credit reporting agency] … It is no wonder that many consumers become confused by the process.[84]

55.67 The Consumer Action Law Centre submitted that, while this 'merry-go-round' is made possible by provisions of the *Credit Reporting Code of Conduct*, 'ultimately it occurs because the OPC does not use its discretion to accept complaints … nor accept that a complaint made to a [credit reporting agency] has been made to the respondent'.[85]

55.68 The Centre proposed minor changes to the Code, and possibly to the *Privacy Act*, to recognise that complaints may be made to a credit provider or a credit reporting agency:

> If a complaint was made to a [credit reporting agency], or a credit provider referred a complaint to a [credit reporting agency], the [credit reporting agency's] role would then be to assess and determine a complaint as between the consumer and the credit provider. If a [credit reporting agency] was unable to resolve a dispute, it could refer the consumer to either the OPC or the EDR scheme to which it is a member.[86]

55.69 The OPC supported requirements that individuals complain to the respondent before making a complaint to the OPC.[87] The ALRC agrees that credit reporting agencies and credit providers should deal with complaints in the first instance. As discussed in Chapter 45, such a requirement is consistent with other legislative complaint-handling regimes and with the terms of most EDR schemes.

55.70 The OPC acknowledged, however, that the complaints process in relation to credit reporting 'may sometimes be confusing for complainants' and that individuals could be better informed about where to direct an initial complaint. The OPC submitted that the complaint-handling process could be improved by amending the credit reporting provisions to include a requirement that complaint-handling information must be included with notices provided to individuals before their information is passed to a credit reporting agency; and when a credit reporting agency records adverse information about them.[88]

---

84 Ibid.

85 Ibid.

86 Ibid. The Act itself, in the Centre's view, might be amended to clarify that a consumer who has already made a complaint to the credit reporting agency has complained to the 'respondent'.

87 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

88 Office of the Privacy Commissioner, *Submission PR 281,* 13 April 2007.

ALRC's view

55.71 Under the *Credit Reporting Code of Conduct*, credit reporting agencies are responsible for resolving disputes between consumers and credit providers.[89] Notably, the Code provides that 'a credit provider should refer to a credit reporting agency for resolution a dispute between that credit provider and an individual where the dispute concerns the contents of a credit report issued by the credit reporting agency'.[90]

55.72 A focus on complaint handling by credit reporting agencies may be seen as 'logical given their central role in the credit reporting system'[91] but creates problems in practice. First, where a credit provider considers that information it disclosed to the agency is accurate, the credit reporting agency has limited capacity to 'look behind' the listing of its subscriber credit provider. Arguably, credit reporting agencies cannot resolve credit reporting complaints that require a determination of rights in specific consumer credit contexts. Secondly, an agency's commercial interests may conflict with the need to make decisions that may affect adversely the interests of its subscribers.

55.73 In contrast to what is stated in the *Credit Reporting Code of Conduct*, credit reporting agencies should refer complaints about the content of credit reporting information provided to the agency by a credit provider to that credit provider for initial dispute resolution. As currently set out in the explanatory notes to the Code, credit reporting agencies should be able to nominate an officer at each credit provider as the first point of contact for the handling of credit reporting complaints.[92]

55.74 Credit reporting agencies and credit providers need to establish effective complaint-handling mechanisms. In many instances, the involvement of a credit reporting agency and a credit provider will be necessary to deal with a credit reporting complaint. The credit provider may need, for example, to investigate the circumstances of an overdue payment and the credit reporting agency to amend its credit reporting information following the outcome of an investigation. Where credit reporting agencies and credit providers share the handling of a complaint, some potential for a complaint-handling 'merry-go-round' may remain.

55.75 This problem may be addressed, in part, by the provision of appropriate information to complainants about the respective roles of credit reporting agencies and credit providers, and access to EDR and OPC complaint-handling processes. In this context, the ALRC proposes that the *Privacy (Credit Reporting Information) Regulations* provide that notification of adverse credit reports should include information about the avenues of complaint available to the individual if he or she has

---

89 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [3.3]–[3.6].
90 Ibid, [3.3].
91 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.
92 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991), [78B].

a complaint about the collection or handling of his or her credit reporting information.[93]

55.76 In addition, time limits on substantiating disputed credit reporting information and mandated EDR schemes (discussed below) should assist to ensure effective complaint handling for individuals who are contesting adverse credit reporting information.

Proposal 55–4 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that:

(a) credit reporting agencies and credit providers must handle credit reporting complaints in a fair, efficient and timely manner;

(b) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint;

(c) a credit reporting agency should refer to a credit provider for resolution of a complaint about the content of credit reporting information provided to the agency by that credit provider; and

(d) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint it must immediately inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

Proposal 55–5 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

93 The ALRC also proposes that, at or before the time credit reporting information is collected, credit providers must ensure that the individual is aware of, among other things, the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her credit reporting information: See Proposal 52–9.

External dispute resolution

55.77 In IP 32, the ALRC asked about the role of external dispute resolution schemes in resolving credit reporting complaints.[94] The ALRC noted that suggestions for reform of the system for handling credit reporting complaints included that an industry-funded EDR scheme be established; and credit providers only be allowed access to the credit reporting system on demonstrating that they have satisfactory internal dispute resolution procedures and are members of the EDR scheme.[95]

55.78 As discussed above, many credit providers are already members of industry EDR schemes, notably those involving the BFSO and TIO. Veda Advantage, the leading consumer credit reporting agency, is also a member of the BFSO.[96] The Consumer Action Law Centre stated that, in its view:

> This gives consumers dealing with Veda Advantage an effective avenue for independent resolution of their complaint (and, we think, a real and effective alternative to the OPC).[97]

55.79 Submissions emphasised the desirability of access to EDR schemes in credit reporting complaint handling.[98] Regulatory requirements that credit providers be members of an EDR scheme were widely supported.

55.80 The Consumer Action Law Centre stated that credit providers should be members of an approved EDR scheme 'given the substantial problems with the current system and difficulties faced by consumers challenging inaccurate or incorrect listings'.[99] Case workers associated with Legal Aid Queensland's Consumer Protection Unit noted that the ASIC requirement for licensed financial services providers to belong to an approved EDR scheme 'has provided positive outcomes for many thousands of consumers who were unable to access court based solutions'.[100]

---

94 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 4–3.

95 Ibid, [4.36].

96 Other credit reporting agencies are not members of an EDR scheme.

97 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

98 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; ANZ, *Submission PR 291,* 10 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; National Legal Aid, *Submission PR 265,* 23 March 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Westpac, *Submission PR 256,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; MasterCard Worldwide, *Submission PR 237,* 13 March 2007; GE Capital Finance Australasia Pty Ltd, *Submission PR 233,* 12 March 2007; Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007; Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007; Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007.

99 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

100 Legal Aid Queensland, *Submission PR 212,* 27 February 2007. See also Queensland Law Society, *Submission PR 286,* 20 April 2007.

55.81 Legal Aid Queensland submitted that all credit providers should belong to an EDR scheme that meets the ASIC standard, before having access to the credit reporting system.[101] The EDR scheme

> should initially determine all complaints by consumers relating to credit reporting, including the power to make a finding regarding the individual's liability for the debt …[102]

55.82 The BFSO suggested that a requirement to belong to an EDR scheme 'could be effected through a licensing system' similar to that under the *Corporations Act*. As many credit providers are already members of the BFSO or other ASIC approved schemes it may be possible

> to utilise the existing framework for external dispute resolution in the financial services sector to facilitate access to an appropriate industry-funded scheme for dispute resolution in the credit reporting industry … The utilisation of existing schemes in the financial services area would also avoid imposing a requirement on credit providers to become members of more than one scheme.[103]

55.83 National Legal Aid suggested that membership of an approved EDR scheme should be included within the definition of a 'credit provider'.[104] Similarly, the CCLC recommended:

> Only credit providers that are required by law to be member of an ASIC approved external dispute resolution scheme (or equivalent benchmark) should be permitted to contribute to, or access credit information from, credit reporting agencies.[105]

55.84 There was also some support for the establishment of a new specialist 'credit reporting ombudsman' to resolve disputes between individuals and credit providers.[106] Others opposed the establishment of any new credit reporting complaint-handling body.[107] The Australian Finance Conference stated that

> the Privacy Commissioner should maintain the role as the facilitator of disputes or complaints under the credit reporting provisions. Industry has a responsibility to have effective complaint handling processes in place, and given the relatively low level of privacy related complaints upheld supports the position that there would be limited value or benefit for the customer or the industry in imposing a further layer of external dispute resolution process in the equation.[108]

---

101 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.
102 Ibid.
103 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.
104 National Legal Aid, *Submission PR 265,* 23 March 2007.
105 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 19.
106 Dun & Bradstreet (Australia) Pty Ltd, *Submission PR 232,* 9 March 2007.
107 Australian Finance Conference, *Submission PR 294,* 18 May 2007; Optus, *Submission PR 258,* 16 March 2007; Min-it Software, *Submission PR 236,* 13 March 2007; Australian Institute of Credit Management, *Submission PR 224,* 9 March 2007.
108 Australian Finance Conference, *Submission PR 294,* 18 May 2007.

55.85 Stakeholders noted the importance of ensuring that any new EDR schemes dealing with credit reporting complaints do not duplicate existing dispute resolution services.[109] Veda Advantage also observed that

> the involvement of multiple parties in complaints resolution is one of the features of information networks, and demonstrates the challenges of effective consumer dispute resolution. The challenge is increased by additional cost each time a new organisation is added into the complaints resolution system.[110]

ALRC's view

55.86 EDR schemes are already a significant feature of credit reporting complaint handling. In particular, many credit providers are members of the BFSO and TIO schemes and Veda Advantage is a member of the BFSO.

55.87 The ALRC agrees with industry and consumer groups that the use of EDR in the handling of credit reporting complaints should be facilitated. The Australasian Retail Credit Association, for example, recommended the implementation of 'consumer complaint, dispute and hardship management procedures that integrate with and fully leverage existing [EDR schemes]'.[111] The Consumer Action Law Centre also noted that encouraging EDR in credit reporting complaint handling is 'consistent with developments in other industry areas, especially related areas such as financial services regulation and more recently, moves to implement such a requirement in the consumer credit arena'.[112]

55.88 The ALRC observes that concerns about the existing regulation of credit reporting have focused as much on how the complaints and enforcement provisions have operated in practice as on the substantive obligations. More effective complaint handling and enforcement is seen by many stakeholders as central in making a significant improvement to the existing regulatory framework. Lack of access to effective complaint-handling mechanisms can have serious consequences for individuals who may have no access to credit while, for example, a disputed default listing remains part of their credit reporting information.

55.89 In Chapter 45, the ALRC makes proposals intended to promote the use of EDR schemes. In credit reporting complaints, it is appropriate that EDR schemes provide the first line of dispute resolution beyond the credit provider or credit reporting agency. Such schemes are funded by industry and understand and have expertise in the commercial environment in which their members operate.

---

109 Confidential, *Submission PR 297,* 1 June 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

110 Veda Advantage, *Submission PR 272,* 29 March 2007.

111 Australasian Retail Credit Association, *Submission PR 218,* 7 March 2007. See also St George Banking Limited, *Submission PR 271,* 29 March 2007.

112 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007. In 2006, the Victorian Government stated that it supports legislating to require all providers of consumer credit in Victoria to subscribe to an alternative dispute resolution scheme: Victorian Government, *Government Response to the Report of the Consumer Credit Review* (2006), 15.

55.90 The ALRC is concerned also to improve OPC conciliation and determination processes and to address the capacity of the OPC to identify and address systemic issues. Placing more of the frontline complaint-handling burden on EDR schemes should assist in achieving these aims.

55.91 The ALRC proposes, therefore, that the *Privacy (Credit Reporting Information) Regulations* provide that credit providers may only list overdue payment information where the credit provider is a member of an EDR scheme approved by the OPC. An alternative approach would be to make membership of an EDR scheme a precondition to any participation in the credit reporting system, rather than to the listing of overdue payment information. Dispute resolution seems needed most in relation to adverse listings. Membership of an EDR scheme can be expensive. The compliance burden may not justify imposing EDR obligations on credit providers who may, for example, wish to obtain credit reports in order to help decide whether to provide goods or services on credit, but do not list defaults.[113]

55.92 The OPC could be expected to approve those EDR schemes already approved by ASIC under the *Corporations Act* and those with another statutory basis, such as the TIO.[114] More broadly, the OPC could look at the ASIC standards[115] and other similar instruments for benchmarks in its approval process.

Proposal 55–6 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where the credit provider is a member of an external dispute resolution scheme approved by the Office of the Privacy Commissioner.

Time limits on disputed credit reporting information

55.93 In IP 32, the ALRC noted that in the United States, under the FCRA,[116] if the completeness or accuracy of information is disputed by a consumer, the credit reporting agency must conduct an investigation and, if not verified, the information must be deleted within 30 days.[117]

113 The separate issue of reciprocity obligations is considered in Ch 51.
114 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).
115 Australian Securities and Investments Commission, *Approval of External Complaints Resolution Schemes: ASIC Policy Statement 139*, 8 July 1999.
116 *Fair Credit Reporting Act 1970* 15 USC § 1681 (US) s 1681i.
117 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), [4.32].

55.94 All stakeholders who addressed the issue in submissions were in favour of requiring credit reporting agencies and credit providers to verify the accuracy of disputed credit reporting within a certain time period or delete the information.[118]

55.95 The Australian Privacy Foundation stated that it supported 'placing the burden of proof in relation to disputed listings more explicitly on the credit provider' and submitted that there should be a 'statutory moratorium on listing while a disputed debt is being resolved within an appropriate court or external dispute resolution (EDR) scheme'.[119] Similarly, the Consumer Law Action Centre submitted that:

> Disputed listings should be removed from credit information files pending resolution of the dispute. To allow them to remain on the file is unfairly prejudicial to the consumer's interests and pre-empts the resolution of the dispute.[120]

55.96 The CCLC made detailed recommendations on the procedures that should apply to the listing of disputed debts. It recommended:

> The onus of proof should be on the credit provider making a listing on a person's credit report to prove the accuracy of that information. If a person notifies a credit reporting agency that information held about that person is disputed, the credit reporting agency should correct the report if possible, or mark the listing as disputed and give credit provider who has listed the information 30 days to provide proof that the debt is owed. If the credit provider fails to provide satisfactory proof within 30 days, the listing should be removed.[121]

55.97 The CCLC also recommended that, where a credit provider has produced prima facie evidence that a listing is correct, and the individual concerned continues to dispute the listing, the credit reporting agency should either:

- Determine the dispute within 30 days on the evidence provided and remove the listing or not accordingly (for example where a person has provided evidence that they did not enter the contract in question, or provides proof of previous settlement or payment in full); or
- Refer the dispute to a dispute resolution scheme with appropriate jurisdiction (for example where a person raises a defence under the

---

118 Legal Aid Queensland, *Submission PR 292,* 11 May 2007; Queensland Law Society, *Submission PR 286,* 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 16; J Codrington, *Submission PR 81,* 2 January 2007.

119 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007. Also N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

120 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

121 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 16.

> Consumer Credit Code which the credit reporting agency does not have the expertise or jurisdiction to determine the dispute).[122]

ALRC's view

55.98 The CCLC noted that a listing may be in dispute because

> either liability is itself in dispute (for example, mistaken identity and contractual disputes), or the consumer had no notice of the obligation and no opportunity to pay through no fault of their own (for example, creditor billing errors) …[123]

55.99 At present, individuals effectively have the burden of showing that a disputed debt is listed improperly because the listing will remain part of their credit reporting information until this is shown. The ALRC considers that this position is unfair given the relative positions of credit providers and individual consumers who may, for example, never have received a utilities bill.[124]

55.100 There should be an obligation on a credit provider to verify disputed credit reporting information. The ALRC proposes that if evidence substantiating the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned. This will provide an incentive for appropriate record-keeping practices and speedy dispute resolution by credit providers and credit reporting agencies.

55.101 Where information is documented adequately by the credit provider, but remains disputed by the individual, the complaint should be referred to an industry-based EDR scheme or the OPC for resolution.

Proposal 55–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers have an obligation to provide evidence to individuals and dispute resolution bodies to substantiate disputed credit reporting information, such as default listings, and that if the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned.

---

122 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 17.

123 Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), 106.

124 See Energy and Water Ombudsman NSW, *Submission PR 225,* 9 March 2007; Telecommunications Industry Ombudsman, *Submission PR 221,* 8 March 2007.

Penalties

55.102 In IP 32, the ALRC asked whether the range of penalties and remedies available to enforce rights and obligations under the credit reporting provisions of the *Privacy Act* should be changed.[125]

55.103 As discussed in Chapter 49, Part IIIA creates a wide range of credit reporting offences. These include, for example, offences in relation to:

- credit providers using or disclosing personal information contained in credit reports other than as permitted;[126]
- credit reporting agencies or credit providers intentionally giving out a credit report that contains false or misleading information;[127]
- persons intentionally obtaining unauthorised access to credit information files or credit reports;[128] and
- persons obtaining access to credit information files or credit reports by false pretences.[129]

55.104 A range of views about penalties were expressed in submissions. Some stakeholders considered that the existing penalties are sufficiently broad or opposed any new penalty provisions.[130] Other stakeholders favoured the introduction of new civil or administrative penalties.[131]

55.105 The Consumer Action Law Centre expressed concern about the 'lack of flexible remedies and appropriate penalties and lack of enforcement action' in relation to credit reporting obligations. The Centre suggested that

> a range of new and flexible remedies should be considered for introduction into the Act. This would greatly assist in allowing the regulatory scheme to be properly implemented as intended … In particular, we consider that a broader range of civil and administrative remedies should be inserted into the Act to give the regulator options for dealing with different sorts of breaches in a flexible and proportionate manner.[132]

---

125 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006), Question 4–4.
126 *Privacy Act 1988* (Cth) ss 18L(2), 18N(2).
127 Ibid s 18R(2).
128 Ibid s 18S(3).
129 Ibid s 18T.
130 Optus, *Submission PR 258,* 16 March 2007; National Credit Union Association Inc, *Submission PR 226,* 9 March 2007.
131 Queensland Law Society, *Submission PR 286,* 20 April 2007; N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.
132 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

55.106 The CCLC also recommended that there should be a wider range of penalties and remedies

> including but not limited to civil penalties (for individual complainants and systemic breaches), injunctions and adverse publicity orders to ensure that there are sufficient incentives for compliance, and adequate responses to noncompliance.[133]

55.107 The Consumer Law Action Centre stated that criminal penalties 'remain appropriate for the worst breaches, as reflected in the Act'.[134] Other stakeholders, however, questioned the utility of the existing offence provisions.[135] The Australian Privacy Foundation, for example, favoured

> the replacement of most of the criminal offence provisions in the Act with a strict liability civil penalty regime. The burden of proof required for successful criminal prosecutions is too high to be a realistic deterrent—we note that there have been no prosecutions to date under Part IIIA. Civil penalty regimes have proved far more effective for enforcement of financial services and consumer protection laws.[136]

55.108 Waters added that the current inclusion of criminal offence provisions in the *Privacy Act* is not consistent with the general approach to enforcement of information privacy laws through a strict liability civil penalty regime.[137]

55.109 Members of the Queensland Law Society also suggested the introduction of a new penalties regime for breaches of the credit reporting provisions and failure to report systemic breaches.[138] American Express stated, in the context of more comprehensive credit reporting, that privacy protection might be strengthened through the introduction of summary infringement notices issued by the OPC.[139]

55.110 Some stakeholders referred to the need for more effective avenues for compensation.[140] The BFSO suggested, for example, that the *Privacy Act* should provide that credit providers and credit reporting agencies are liable for 'financial and non-financial' loss to individuals 'demonstrated to have flowed from an error in listing'.[141]

---

133 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007; Consumer Credit Legal Centre (NSW) Inc, *Credit Reporting Research Report* (2007), rec 53.

134 Consumer Action Law Centre, *Submission PR 274,* 2 April 2007.

135 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007; Australian Privacy Foundation, *Submission PR 275,* 2 April 2007; Consumer Action Law Centre, *Submission PR 274,* 2 April 2007; Consumer Credit Legal Centre (NSW) Inc, *Submission PR 255,* 16 March 2007.

136 Australian Privacy Foundation, *Submission PR 275,* 2 April 2007.

137 N Waters—Cyberspace Law and Policy Centre UNSW, *Submission PR 277,* 3 April 2007.

138 Queensland Law Society, *Submission PR 286,* 20 April 2007.

139 American Express, *Submission PR 257,* 16 March 2007.

140 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007; American Express, *Submission PR 257,* 16 March 2007.

141 Banking and Financial Services Ombudsman Ltd, *Submission PR 263,* 21 March 2007.

ALRC's view

55.111 Part IIIA creates a wide range of credit reporting offences. The extent to which these should be retained or replaced is dependent, in large part, on the ALRC's ultimate recommendations with respect to penalties under the *Privacy Act* generally. In Chapter 46, the ALRC proposes that the *Privacy Act* should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual.[142]

55.112 The ALRC understands that no prosecutions have ever been launched under the credit reporting offence provisions. At least some of the relevant conduct is covered, in any case, by other offences under Commonwealth legislation. The *Criminal Code*, for example, creates an offence in respect to unauthorised access to, or modification of, data held in a computer to which access is restricted.[143]

55.113 Since the enactment of the credit reporting provisions, civil penalty regimes have become a more common means to enforce consumer protection laws including, for example, under the financial services civil penalty provisions of the *Corporations Act*[144] and the uniform *Consumer Credit Code*.[145] The ALRC considers that a civil penalty regime is a more appropriate enforcement mechanism for breaches of credit reporting regulation than the suite of criminal offences currently provided for in the Act.

Proposal 55–8 The *Privacy Act* should be amended to:

(a) remove the credit reporting offences by repealing ss 18C(4), 18D(4), 18K(4), 18L(2), 18N(2), 18R(2), 18S(3) and 18T; and

(b) allow a civil penalty to be imposed where there is a serious or repeated breach of the proposed *Privacy (Credit Reporting Information) Regulations*.

142 Proposal 46–2.
143 *Criminal Code Act 1995* (Cth) s 478.1.
144 *Corporations Act 2001* (Cth) ss 1317DA, 1317E(1)(ja)–(jg).
145 *Consumer Credit Code* pt 6. The *Consumer Credit Code* is set out in the *Consumer Credit (Queensland) Act 1994* (Qld) and is adopted by legislation in other states and territories.

56. Regulatory Framework for Health Information

Contents

Introduction 1559
National consistency 1561
Issues and problems 1561
A proposed solution 1565
A separate set of Health Privacy Principles? 1570
Electronic health information systems 1581
Health*Connect* and NEHTA 1582
Medicare and Pharmaceutical Benefits 1589

Introduction

56.1 In 2004, the Australian Government Department of Health and Ageing (DOHA) stated that:

> Privacy is a fundamental principle underpinning quality health care. Without an assurance that personal health information will remain private, people may not seek the health care they need which may in turn increase the risks to their own health and the health of others. Indeed consumers regard health information as different to other types of information and consider it to be deeply personal.[1]

56.2 The personal health information of health consumers was traditionally protected by the ethical and legal duties of confidentiality. These duties are owed by health service providers—such as doctors, dentists, nurses, physiotherapists and pharmacists—to health consumers and prevent the use of personal health information for a purpose that is inconsistent with the purpose for which the information was provided. A legal duty of confidentiality may arise in equity, at common law or under contract. Health service providers are also often subject to confidentiality provisions in professional codes of conduct[2] and, if they are employed in the public sector, also may be subject to legislative secrecy provisions.

---

1 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

2 See, eg, Australian Medical Association, *Code of Ethics* (2004), s 1.1(l). Confidentiality is also discussed in Chs 5, 12 and 57.

56.3 Duties of confidentiality recognise the dignity and autonomy of the individual,[3] as well as the public interest in fostering a relationship of trust between health service providers and health consumers to ensure both individual and public health outcomes.[4] Such duties are not absolute and there are circumstances in which the law permits, and sometimes requires, the disclosure of confidential personal health information.[5]

56.4 Where legislation establishes health agencies or provides the basis for health related functions to be carried out, officers of those agencies and others performing functions under the legislation frequently are subject to secrecy provisions that prohibit them from disclosing personal information about third parties except in the course of their duties.[6] There is also a range of disease-specific legislation that may include provisions intended to protect individuals' health information. For example, legislation dealing with HIV/AIDS generally requires the use of codes to link test results with individuals rather than including personal details on test request forms.[7]

56.5 More recently, privacy legislation has been introduced in a number of Australian jurisdictions specifically to regulate the handling of personal health information.[8] An overview of privacy regulation in the states and territories, including health privacy regulation, is provided in Chapter 2. Health service providers continue to be subject to secrecy provisions and duties of confidentiality. Although the regimes exist side by side, Marilyn McMahon has suggested that:

> In practice the less costly, more 'user friendly' complaint procedures offered under the privacy regimes may in fact mean that they increasingly 'cover the field' and that the traditional, common law remedies for protecting confidentiality become archaic.[9]

56.6 In its submission, DOHA noted the following changes to the health services context that may have implications for the way that health information is handled:

> There is an increasing focus on coordinated multi-team care through a mix of public and private providers. In delivering healthcare services in this environment, a large volume of information about individuals moves frequently between the public and private sectors, and across State and Territory boundaries. To provide an indication of the volume and frequency of these communications, there were 4.2 million in-patient

---

3 M McMahon, 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes & Dilemmas in Health Law* (2006) 563, 579.

4 P Finn, 'Confidentiality and the "Public Interest"' (1984) 58 *Australian Law Journal* 497, 502.

5 See, eg, *Public Health Act 1991* (NSW) s 14; *Health Act 1958* (Vic) s 138 in relation to notifiable diseases. See also the discussion of professional confidential relationship privilege in Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [15.3]–[15.14], [15.31]–[15.44].

6 See, eg, *National Health Act 1953* (Cth) s 135A; *Health Insurance Act 1973* (Cth) s 130; *Health Administration Act 1982* (NSW) s 22; *Health Services Act 1988* (Vic) s 141.

7 R Magnusson, 'Australian HIV/AIDS Legislation: A Review for Doctors' (1996) 26 *Australian & New Zealand Journal of Medicine* 396.

8 *Privacy Act 1988* (Cth); *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Personal Information Protection Act 2004* (Tas); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act 2002* (NT).

9 M McMahon, 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes & Dilemmas in Health Law* (2006) 563, 583.

> discharges from public hospitals in 2003/04, with about one-half of these being on the 'same-day'. A number of information exchanges between providers in the public and private sectors may have been associated with each of these discharges, including for referral, discharge or enquiry with a patient's GP, and with contracted pathology or radiology diagnostic services.[10]

56.7 Technology is developing to help deal this challenge. DOHA went on to note that:

> Australia is on the threshold of major developments in national e-health systems and the use of telehealth services. The aim of these systems is to enable health information to be shared more reliably, securely and efficiently between healthcare providers with the aim of delivering safe care and better health outcomes for individuals. The use of these systems will increase the volume and frequency of communications and may mean the individual whom the information concerns is located in a different State or Territory to the holder of the information. New work systems and practices will emerge as e-health systems are developed and implemented, and the use of telehealth services expand.[11]

56.8 In this chapter, the ALRC considers how to meet these challenges, while ensuring that individuals' health information is handled appropriately. The chapter considers the need for greater national consistency in health privacy regulation as well as nationwide developments in relation to electronic health information systems. The consideration of national consistency in health privacy regulation is closely related and cross refers to the discussion of national consistency in privacy regulation more generally in Chapter 4.

National consistency

Issues and problems

56.9 Chapter 2 provides an overview of privacy regulation in Australia. The position is particularly complex in the area of health information for a number of reasons. In general terms, the *Privacy Act* regulates the handling of health information in the Australian Government and ACT public sectors and in the private sector. As noted above, a number of the states and territories also have passed legislation that regulates the handling of health information in the state or territory public sector and/or the private sector.[12] The following table provides a general view of the jurisdictional scope of some of the major pieces of health privacy legislation in Australia.

---

10 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

11 Ibid.

12 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Personal Information Protection Act 2004* (Tas); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act 2002* (NT). Other state and territory legislation may also impact on the handling of health information, for example, the New South Wales Government Department of Health, *NSW Health Privacy Manual (Version 2)* (2005) includes information on the *Health Administration Act 1982* (NSW); *Mental Health Act 1990* (NSW); *Public Health Act 1991* (NSW); *State Records Act 1989* (NSW); and the *Freedom of Information Act 1989* (NSW).

Table 56–1: Privacy Legislation Regulating the Handling of Health Information		
Jurisdiction	**Public Sector**	**Private Sector**
Commonwealth	*Privacy Act 1988 (Cth)*	*Privacy Act 1988* (Cth)
New South Wales	*Health Records and Information Privacy Act 2002 (NSW)*	*Health Records and Information Privacy Act 2002* (NSW) *Privacy Act 1988* (Cth)
Victoria	*Health Records Act 2001 (Vic)*	*Health Records Act 2001 (Vic)* *Privacy Act 1988* (Cth)
Queensland	[See 56.10 below]	*Privacy Act 1988* (Cth)
Western Australia	[See 56.12 below]	*Privacy Act 1988* (Cth) [See also 56.12 below]
South Australia	[See 56.11 below]	*Privacy Act 1988* (Cth)
Tasmania	*Personal Information Protection Act 2004* (Tas)	*Privacy Act 1988* (Cth)
ACT	*Health Records (Privacy and Access) Act 1997* (ACT) *Privacy Act 1988* (Cth)	*Health Records (Privacy and Access) Act 1997* (ACT) *Privacy Act 1988* (Cth)
Northern Territory	*Information Act 2002* (NT)	*Privacy Act 1988* (Cth)

56.10 Although there is no specific privacy legislation regulating the handling of health information in the public sector in Queensland, Western Australia or South Australia, such information may be protected in other ways. In Queensland, the state government has introduced a privacy policy by administrative, rather than legislative means. *Information Standard 42 on Information Privacy*[13] is based on the Information Privacy Principles (IPPs) and *Information Standard 42A on Information Privacy for*

13 Queensland Government, *Information Standard 42—Information Privacy* (2001).

the Queensland Department of Health[14] is based on the National Privacy Principles (NPPs). Both standards are issued under the *Financial Management Standard 1997* (Qld).

56.11 In South Australia, the state government has also introduced a privacy policy by administrative, rather than legislative means. The *PC012—Information Privacy Principles Instruction* is based on the IPPs. The Department of Health *Code of Fair Information Practice* is based on the NPPs.

56.12 In Western Australia, no legislation or formal administrative arrangements are currently in place. The Information Privacy Bill 2007, however, was introduced into the Western Australian Parliament on 28 March 2007. The Bill proposes to regulate the handling of personal information in the state public sector and the handling of health information in the public and private sectors.[15] The Bill contains a set of eight Information Privacy Principles and 10 Health Privacy Principles.

56.13 As indicated in Table 56–1 above, both a federal Act and a state or territory Act regulate the handling of health information in the private sector in a number of jurisdictions. The New South Wales *Health Records and Information Privacy Act* and the Victorian *Health Records Act* contain a set of Health Privacy Principles (HPPs). The ACT *Health Records (Privacy and Access) Act* contains a set of Privacy Principles. Private sector health service providers in these jurisdictions are therefore required to comply with two sets of principles: the NPPs in the *Privacy Act* and the relevant set of HPPs or Privacy Principles. While the HPPs in New South Wales and Victoria are based on the NPPs, they are not identical and in some cases impose different standards. The ACT Privacy Principles are based on the IPPs, but have been modified to apply specifically to health information.[16]

56.14 The scope of the state and territory legislation may also differ from the federal legislation. For example, the Victorian *Health Records Act* covers small business operators and employee records—unlike the *Privacy Act*.

56.15 The New South Wales and Victorian HPPs and the ACT Privacy Principles also differ from each other, so that information passing from one jurisdiction to the other may become subject to a different set of rules. This causes particular difficulty for health service providers and researchers operating across jurisdictional borders or nationally.

---

14 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).

15 A related Bill, the Freedom of Information Amendment Bill 2007 (WA), was introduced on the same day. This Bill provides the Privacy and Information Commissioner with powers to resolve FOI complaints by conciliation.

16 Explanatory Memorandum, Health Records (Privacy and Access) Bill 1997 (ACT).

56.16 Another problem arises in jurisdictions like Tasmania, where health information in the public sector is regulated by the *Personal Information Protection Act* and health information in the private sector is regulated by the *Privacy Act.* The *Personal Information Protection Act* contains a set of Personal Information Protection Principles (PIPPs) that are not identical to the NPPs.

56.17 In the health services context, individuals regularly move between public and private sector health service providers. For example, an individual may be referred by a private sector general practice for treatment in a public hospital. In some situations the public and private sector work side by side; for example: where an individual is treated as a private patient in a public hospital; or a research project is conducted on a multi-site basis, across the public sector/private sector divide. This means that health information may be subject to two different sets of privacy principles at the same time.

56.18 Some of the same problems arise because of the distinction in the *Privacy Act* between public sector agencies and private sector organisations. Agencies are bound by the IPPs and organisations are bound by the NPPs. There are circumstances in which an organisation or agency may be subject to both the IPPs and the NPPs. For example, an Australian Government contractor may be bound to comply with the NPPs as an organisation, but will also be bound by contract to comply with the IPPs in relation to information held pursuant to that contract.[17] These issues, including the need for a single set of principles in the *Privacy Act*, are considered in detail in Parts C and D.

56.19 The Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act 1988* (Cth) (the OPC Review) identified the following problems that arise because of this inconsistency and overlap:

- increased compliance costs, particularly where businesses are conducted across jurisdictional boundaries;
- confusion about which regime regulates particular businesses;
- forum shopping to exploit differences in regulation; and
- uncertainty among consumers about their rights.[18]

56.20 In its submission to the OPC Review, DOHA stated that:

> The co-existence of Commonwealth, state and territory health information privacy legislation has created a significant burden on private sector health care services in

---

17 See *Privacy Act 1988* (Cth) s 95B in relation to requirements for Commonwealth contracts; and s 6A(2)—no breach of an NPP if an act or practice of contracted service provider is authorised by a provision of the contract that is inconsistent with the NPP.

18 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 66–68. The costs of legislative inconsistency and regulatory fragmentation are considered in detail in Ch 11.

> understanding and meeting respective obligations, as well as confusion for health consumers affected by dual legislative instruments.[19]

56.21 In relation to health and medical research, the National Health and Medical Research Council (NHMRC) stated in its submission to the OPC Review that:

> There is evidence that legitimate and ethical activities (which in some cases are vital to the quality provision of health care or the conduct of important health and medical research) are being delayed or proscribed because some key decision-making bodies are unable to determine, with sufficient confidence, whether specific collections, uses and/or disclosures of information accord with legislative requirements. The adoption of a highly conservative approach is resulting in excessive administrative effort and a reluctance to approve the legitimate use and disclosure of health information for the purposes of health care, as well as health and medical research.[20]

56.22 Submissions to the OPC Review overwhelmingly expressed the view that the existing state of health privacy laws in Australia was unsatisfactory for health service providers, health and medical researchers and individuals.[21] Concern also was expressed that the problem would get worse as electronic health records become commonplace.[22]

56.23 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the NHMRC recommended that:

> As a matter of high priority, the Commonwealth, States and Territories should pursue the harmonisation of information and health privacy legislation as it relates to human genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.[23]

A proposed solution

56.24 As discussed in Chapter 4, the *Privacy Act* expressly allows state and territory privacy legislation to operate to the extent that it is capable of operating concurrently with the *Privacy Act*. The OPC Review stated that:

> It is not clear whether section 3 of the *Privacy Act*, which provides that the operation of state and territory laws that are 'capable of operating concurrently with' the Act are not to be affected, covers the field or not. This provision determines whether or not a state or territory privacy law, or part of it, is or is not constitutional.

---

19 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

20 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

21 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

22 Ibid, 43.

23 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–1.

> This lack of clarity leaves the way open to a state or territory to pass its own laws on the ground that there is no constitutional barrier to doing so. It certainly may be that state and territory legislation purporting to regulate health records is inconsistent at least to the extent that it imposes obligations on organisations covered by the *Privacy Act*. If so, it may be unconstitutional. Section 3 could be amended to make it clear that the *Privacy Act* was intended to cover the field.[24]

56.25 The OPC recommended that 'The Australian Government should consider amending section 3 of the *Privacy Act* to remove any ambiguity as to the regulatory intent of the private sector provisions'.[25]

56.26 Section 3 of the *Privacy Act* indicates the Australian Parliament's intention that the Act should not 'cover the field' in the constitutional sense and that state and territory legislation should be allowed to operate alongside the *Privacy Act*, to the extent that such laws are not directly inconsistent with the *Privacy Act*. Section 3 also makes clear that, where state and territory law is directly inconsistent with the *Privacy Act*—that is, it is not capable of operating concurrently with the Act—that law will be invalid to the extent of the inconsistency.[26]

Submissions and consultations

56.27 There was strong support in submissions and consultations for greater national consistency in the regulation of health information.[27] The NHMRC expressed the view that:

> the current state of privacy regulation in Australia is entirely unsatisfactory. Its complexity is impacting on the proper provision of health care and the conduct of important health and medical research, in addition to creating significant unnecessary compliance costs.
>
> The NHMRC considers that a solution to the current problem of an unnecessarily complex privacy regulatory regime needs to be identified and implemented as a priority.
>
> The NHMRC supports the development of a national set of privacy principles that apply to all health information uniformly across the public and private sectors.[28]

56.28 A number of insurance bodies discussed the difficulties that overlapping and inconsistent health privacy legislation posed for their national operations.[29] Other

---

24 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 45.

25 Ibid, rec 2.2.

26 Section 109 of the *Australian Constitution* provides that 'When a law of a State is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid'.

27 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108,* 15 January 2007.

28 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

29 AAMI, *Submission PR 147,* 29 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007;

stakeholders expressed concern about the difficulty of conducting research or providing health services across jurisdictional boundaries. It was noted that health consumers often shift between jurisdictions and should receive the same level of protection in every state and territory.[30]

56.29 The New South Wales Guardianship Tribunal noted that:

> It is not uncommon for people with disabilities to receive services from a range of private and government organisations. In many cases, the person's health information may need to be disclosed or collected to enable the appropriate services to be provided. Inconsistencies or complexities in the legal requirements about information handling add to the burden of pressures involved in working in the disability sector.[31]

56.30 The OPC expressed the view that:

> there is a strong need to clarify the application of the Privacy Act to private sector health service providers. Section 3 of the Privacy Act should be amended to make clear that the National Privacy Principles 'cover the field' for the regulation of private sector health service providers. This would address a key source of uncertainty and potential fragmentation in health privacy regulation in Australia.[32]

56.31 A number of stakeholders expressed support for a cooperative approach to achieving national consistency, rather than amending s 3 of the *Privacy Act* to exclude state and territory legislation.[33] The Government of South Australia did not support the Australian Government legislating to 'cover the field', expressing concern about the possibility that the *Privacy Act* might impact adversely on the operation of state legislation dealing with issues such as compulsory notification in relation to child abuse and notifiable diseases.[34]

56.32 The Western Australian Department of Health noted that:

> The regulation of health privacy has extensive implications for performance of State responsibilities in the delivery of health care and the management of health systems and should remain within State control. Significant local issues include:
>
> - the use of health information, for planning, funding and evaluation of health services and for health related research;
> - the management of Clinical Information Systems to facilitate continuity of care; and

---

30 Health Informatics Society of Australia, *Submission PR 196,* 16 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; A Smith, *Submission PR 79,* 2 January 2007; R Magnusson, *Submission PR 3,* 9 March 2006.

31 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007.

32 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

33 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006.

34 Government of South Australia, *Submission PR 187,* 12 February 2007.

- the sharing of information between agencies.[35]

56.33 The Office of the Health Services Commissioner in Victoria expressed the view that state health privacy legislation was important to allow health consumers access to local complaint handling bodies:

> As well as administering the *Health Records Act*, HSC [the Office of the Health Services Commissioner] also handles complaints about health services in Victoria. HSC is therefore familiar with the workings of the local health system. This is very important when handling complaints about possible breaches of health privacy. HSC receives a number of complaints where the person is complaining about the health service they received as well as a breach of health privacy. Both complaints are dealt with together, as there is often an overlap of issues.[36]

ALRC's view

56.34 The importance of national consistency in the handling of personal information is examined in detail in Chapter 4. Although the health information privacy legislation in New South Wales, Victoria and the ACT has highlighted the problems caused by overlapping and inconsistent legislation, the issue is not confined to the handling of health information. The ALRC's main proposals in relation to national consistency are framed in relation to personal information (including health information), and can be found in Chapter 4.

56.35 The ALRC has found that inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance burden and cost and impediments to information sharing and national initiatives in the provision of health services and the conduct of research.[37] The ALRC has concluded that national consistency should be one of the goals of privacy regulation in Australia and that personal information should attract similar protection whether that personal information is being handled by an Australian Government agency, a state or territory government agency or a private sector organisation.

56.36 In Chapter 4, the ALRC proposes that the *Privacy Act* be amended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information in the private sector.[38] In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations: *Health Records and Information Privacy Act 2002* (NSW), *Health Records Act 2001* (Vic), and the *Health Records (Privacy and Access) Act 1997* (ACT).

56.37 Other state and territory laws may be introduced that seek to regulate the handling of personal information or health information in the private sector, for example, the Information Privacy Bill 2007 (WA). The ALRC therefore proposes that

---

35 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.
36 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.
37 See Ch 11.
38 Proposal 4–1.

the *Privacy Act* be amended to allow the making of regulations to exclude such laws, if necessary, in the future.[39]

56.38 The ALRC notes state and territory concerns about the interaction of the proposed amended *Privacy Act* with state and territory laws; for example, state and territory public health Acts requiring health service providers to collect and record certain information about health consumers with notifiable diseases, such as tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[40] Other state and territory laws contain provisions that require mandatory reporting when a child is suspected of being at risk of harm.[41]

56.39 While the proposed Unified Privacy Principles (UPPs) would accommodate most of these laws,[42] to ensure clarity the ALRC proposes that the *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with 'non-excluded matters' set out in the legislation. The Australian Government, in consultation with state and territory governments, should develop a list of specific 'non-excluded matters' for the purposes of the *Privacy Act*.[43]

56.40 In relation to the handling of personal information in the state and territory public sectors, the ALRC proposes an intergovernmental agreement. A major cause of inconsistency in Australian privacy laws is that the *Privacy Act* and state and territory privacy laws include similar, but not identical, privacy principles. It is the ALRC's view that the most effective method of dealing with these inconsistencies is the adoption of identical privacy principles across Australia. The intergovernmental agreement would provide that state and territory privacy legislation apply the proposed UPPs and the proposed *Privacy (Health Information) Regulations*, discussed further below and in Chapter 57, as in force under the *Privacy Act* from time to time.[44]

56.41 In addition, the ALRC proposes that definitions of key terms used in the *Privacy Act* (including 'personal information', 'sensitive information' and 'health information') should be adopted in state and territory privacy legislation.[45] The ALRC does not propose that the states and territories be required to develop legislation that exactly mirrors the *Privacy Act*. Apart from the specified elements, the states and territories would be free to develop legislation in relation to their public sectors that

---

39 Proposal 4–2.
40 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.
41 See, eg, *Children, Youth and Families Act 2005* (Vic) pt 4.4; *Child Protection Act 1999* (Qld); *Children's Protection Act 1993* (SA) pt 4; *Children Young Persons and Their Families Act 1997* (Tas) pt 3.
42 Under, eg, the exception to the 'Use and Disclosure' principle for use and disclosure that is 'required or authorised by or under a law'.
43 Proposal 4–3.
44 Proposal 4–4.
45 Proposal 4–4.

accommodates existing state and territory information laws and compliance and enforcement mechanisms.

56.42 In Chapter 45 it is proposed that the *Privacy Act* be amended to allow the Privacy Commissioner to delegate his or her powers, including the power to handle complaints, to state and territory authorities.[46] For example, complaints against private sector health service providers in Victoria are currently handled by either the OPC or the Victorian Health Services Commissioner. The proposals discussed above would remove this jurisdiction from the state body. The ALRC recognises, however, that there are advantages to handling complaints at a local level. The local complaint handler often has contacts and relationships with local providers, and is in a better location to conduct conciliation conferences. Proposal 45–3 would allow the Privacy Commissioner to enter into an agreement with, for example, the Victorian Health Services Commissioner to allow the state body to handle complaints against Victorian private sector health service providers under the *Privacy Act*.

Proposal 56–1 The Privacy Commissioner should consider delegating the power to handle complaints under the *Privacy Act* in relation to interferences with health information privacy by organisations to state and territory health complaint agencies.

A separate set of Health Privacy Principles?

56.43 At the federal level, health information is generally treated as a sub-set of 'sensitive information' under the *Privacy Act*, although there are a number of provisions and principles that deal specifically with 'health information'. As noted above, three of the states and territories have taken a different approach. New South Wales, Victoria and the ACT have separate legislation—including a separate set of privacy principles—dealing specifically with health information.[47]

56.44 In considering the Privacy Amendment (Private Sector) Bill 2000 (Cth), the House of Representatives Standing Committee on Legal and Constitutional Affairs noted that the inclusion of health information was the most contentious aspect of the Bill.[48] Some stakeholders expressed the view that health information should not be included in the Bill because the:

- health sector is so different from other sectors that the attempt to incorporate it within the general framework of the Bill was misguided;

---

46 Proposal 45–3.

47 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

48 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [6.2].

- rights contained in the Bill enabling individuals to access their own health information were inadequate; and

- Bill created inconsistent standards governing privacy rights in the public and private sectors.[49]

56.45 Other stakeholders expressed the view that health information should be included in the Bill on the basis that health information is held in a variety of contexts other than the health services context—such as insurance and employment—and that a different approach to the handling of health information would make it difficult to achieve a nationally consistent privacy framework. In addition, stakeholders expressed the view that the modifications made in relation to the handling of sensitive information in the NPPs provided an appropriate and workable framework for the handling of health information.[50]

56.46 The House of Representatives Standing Committee concluded that health information should be included in the Bill.[51] The Committee expressed concern, however, about 'the resulting plethora of principles that will then apply to both the public and private health sectors'.[52] The Committee recommended that:

> the Government encourage all relevant parties to reach an agreed position on the major issues raised in the evidence to this inquiry, such as the harmonisation of privacy principles applicable to the public and private sectors, as a matter of urgency.[53]

56.47 The issue of national consistency was central to these recommendations, but the Committee did not consider in any detail the argument that health information and the health context are so unique that they require a separate set of principles.

The Privacy Act 1988 (Cth)

56.48 As discussed in Chapter 3, the federal *Privacy Act* originally regulated the handling of personal information by Australian Government and ACT public sector agencies. The Act required agencies to apply the IPPs in handling all personal information, including health information. The IPPs do not draw a distinction between personal information and health information.[54]

56.49 The *Privacy Amendment (Private Sector) Act 2000* (Cth) and the NPPs set out in that Act, however, do draw a distinction between personal information and 'sensitive

---

49 Ibid, [6.12].
50 Ibid, [6.7]–[6.10].
51 Ibid, rec 15.
52 Ibid, [6.35].
53 Ibid, rec 14.
54 The IPPs and NPPs are discussed in detail in Part D of this Discussion Paper.

information'. Sensitive information is defined to include 'health information about an individual' and is given a higher level of protection under the NPPs in the following ways. Sensitive information:

- may be collected only with consent, except in specified circumstances;[55]
- must not be used or disclosed without consent for a secondary purpose unless that purpose is directly related to the primary purpose of collection;[56]
- must not be used without consent for the secondary purpose of direct marketing;[57] and
- cannot be shared by 'related bodies corporate' in the same way that they may share other 'personal information'.[58]

56.50 The NPPs also make special and specific provision for the collection, use and disclosure of health information in some circumstances; for example, for the management, funding and monitoring of a health service and for the purposes of research, or the compilation of statistics, relevant to public health or public safety. The management, funding and monitoring of health services is discussed in Chapter 57 and research is discussed in detail in Chapter 58.

56.51 In addition, NPP 10.2 provides for the collection of health information without consent where the information is necessary to provide a health service to the individual. The information must only be collected as required or authorised by or under law, or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the organisation.[59]

56.52 NPP 2.1(ea) deals specifically with genetic information that has been collected in the course of providing a health service to an individual and allows an organisation to use or disclose that information to a genetic relative where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative. NPP 2.1(ea) also provides that any such use or disclosure must be in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner.[60]

---

55 *Privacy Act 1988* (Cth) NPP 10.
56 Ibid NPP 2.1(a).
57 Ibid NPP 2.1(c).
58 Ibid s 13B.
59 NPP 10.2 is discussed further in Ch 57.
60 This provision implements Rec 21–1 of Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003). NPP 2.1(ea) is discussed further in Ch 57.

56.53 NPP 2.4 establishes a regime under which a health service provider may disclose an individual's health information to 'a person who is responsible for the individual' including certain family members, carers and legal guardians in some circumstances. These include where the individual is physically or legally incapable of giving consent to the disclosure.[61]

56.54 NPP 6.1(b) provides a special exception to the access principle in relation to health information. An organisation need not provide access to an individual's health information where providing access would pose a serious threat to the life or health of any individual. In these circumstances the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.[62]

The draft National Health Privacy Code

56.55 In June 2000, Australian Health Ministers established the Australian Health Ministers' Advisory Council (AHMAC) National Health Privacy Working Group. The purpose of the Working Group was to address the need for a nationally consistent framework for health information privacy. The AHMAC Working Group was made up of representatives of state and territory health authorities and the Australian Government Attorney-General's Department and was chaired by DOHA. The Health Insurance Commission, the Australian Institute of Health and Welfare and the OPC had observer status on the AHMAC Working Group and provided specialist advice.[63]

56.56 The framework developed by the AHMAC Working Group has become known as the draft *National Health Privacy Code*. In order to achieve national consistency, the draft Code was intended to apply to all health service providers and organisations that collect, hold or use health information across the public and private sectors in every Australian state and territory.[64] The draft Code contains 11 National Health Privacy Principles (NHPPs) and additional detailed procedures for providing individuals with access to their health information.

56.57 Following a public consultation process, a revised version of the Code, draft mandatory research guidelines and explanatory notes for the use or disclosure of genetic information were developed.[65] These have not, however, been made publicly available. Consequently, where provisions of the draft Code are discussed in this Discussion Paper, references are to the provisions of the draft Code released for public comment in 2003. While much of the content of the draft Code was finalised, as at

---

61 NPP 2.4 is discussed further in Ch 57 and Ch 61 in relation to adults with a decision-making disability.

62 NPP 6.1(b) is discussed further in Ch 57.

63 Phillips Fox, *Report on Public Submissions in Relation to Draft National Health Privacy Code* (2003), 1.

64 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 1 cl 1, pt 2 div 2.

65 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

August 2006, it had not been formally endorsed at ministerial level[66] and an implementation mechanism had not been settled.[67]

56.58 Although the NHPPs have much in common with the NPPs, there are also numerous differences. In general, the NHPPs are more detailed and provide specific guidance on issues such as the handling of health information on the death of a health service provider or where a health service closes, is sold or amalgamates with another service. Some specific NHPPs differ from their equivalent NPPs. For example, while NPP 4 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed,[68] NHPP 4 requires health service providers to retain health information for at least seven years.[69]

State and territory health privacy legislation

56.59 The *Health Records and Information Privacy Act 2002* (NSW) regulates the handling of health information in the public and private sectors and includes a set of 15 Health Privacy Principles (HPPs). The HPPs expressly address issues such as: the use of health information without consent for the funding, management, planning or evaluation of health services;[70] for research;[71] and health records linkage.[72] The Act also includes detailed provisions on providing access to health information.

56.60 The *Health Records Act 2001* (Vic) also regulates the handling of health information in the public and private sectors and includes a set of 11 HPPs. The Victorian HPPs require the retention of health information records for at least seven years.[73] The HPPs also expressly address issues such as: the use of health information without consent in the funding, management, planning, monitoring, improvement or evaluation of health services;[74] the use of health information in research;[75] the transfer of health information when the consumer changes health service provider; and arrangements for the custody of health information when a health service provider closes.[76] As in New South Wales, the Act includes detailed provisions on providing access to health information.

56.61 The ACT *Health Records (Privacy and Access) Act 1997* regulates the handling of health information in the public and private sectors and includes a set of 12 Privacy Principles. These principles expressly address issues such as: the sharing of

---

66 Australian Government Department of Health and Ageing, *Correspondence*, 17 August 2006.
67 National E-Health Transition Authority, *NEHTA's Approach to Privacy*, Version 1.0 (2006).
68 *Privacy Act 1988* (Cth) sch 3, NPP 4.2.
69 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 4.2.
70 *Health Records and Information Privacy Act 2002* (NSW), sch 1, HPP 10(1)(d).
71 Ibid sch 1, HPP 10(1)(f).
72 Ibid sch 1, HPP 15.
73 *Health Records Act 2001* (Vic) sch 1, HPP 4.
74 Ibid sch 1, HPP 2.2(f).
75 Ibid sch 1, HPP 2.2(g).
76 Ibid sch 1, HPP 10.

information among members of a treating team;[77] transfer or closure of a health service provider's practice; and the transfer of a health consumer's health information from one health service provider to another when the consumer changes health service provider.[78] In common with New South Wales and Victoria, the Act includes detailed provisions on providing access to health information.

Submissions and consultations

56.62 In consultation, the Office of the Health Services Commissioner in Victoria expressed the view that health information does require a separate set of principles because of the intimate nature of the information and the fact that some health information—such as mental health information—can lead to stigmatisation or discrimination.[79] In its submission, the Office of the Health Services Commissioner also expressed the view that the draft *National Health Privacy Code* provided a good starting point:

> A great deal of important work and consultation with key stakeholders has already taken place. It would be a regrettable waste of public resources not to utilize the work involved in drafting the *National Code*. Mirror or applied legislation as set out in paragraph 8.43 of the Issues Paper are the most desirable and effective models for implementing the *National Code*.[80]

56.63 A number of other stakeholders agreed that health information and the health services context are unique and require a specific regulatory regime.[81] Support was also expressed for the draft *National Health Privacy Code.*[82]

56.64 The Australian Nursing Federation stressed the need for consistent and carefully crafted principles to assist health service providers to achieve the difficult balances that come up in their daily decision making. The Federation also noted the considerable investment in the development of the draft *National Health Privacy Code* and

---

77 *Health Records (Privacy and Access) Act 1997* (ACT) sch 1, Privacy Principles 9 and 10.

78 Ibid sch 1, Privacy Principles 11 and 12.

79 Victorian Government Office of the Health Services Commissioner, *Consultation PC 28*, Melbourne, 9 May 2006.

80 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

81 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Health Informatics Society of Australia, *Submission PR 196,* 16 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

82 Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

expressed the view that the Code was an appropriate vehicle for developing a nationally consistent framework for the regulation of health information.[83]

56.65 The Centre for Law and Genetics[84] and the Caroline Chisholm Centre for Health Ethics referred to the need to gather familial and social information, including genetic health information, in the health services context:

> The relevant professional should be afforded the appropriate freedom and discretion to responsibly record such information and detail, without fear that there has been a breach of privacy. We believe the general privacy principles do not adequately accommodate such information handling and recording, transfer and sharing.[85]

56.66 The Western Australian Department of Health expressed support for a separate set of health principles, noting the need to use health information for continuity of care in relation to individuals and monitoring and protecting the community on public health issues. The Department noted, however, that a separate set of principles may lead to uncertainty in some contexts—such as child welfare—about which principles apply.[86]

56.67 Other stakeholders were of the view that, for simplicity and consistency, one set of privacy principles should apply to personal information, including health information. There was recognition, however, that there may be a need for supplementary principles or guidance on the detailed application of the principles in the health services context.[87]

56.68 The NHMRC expressed some support for the draft *National Health Privacy Code,* but stated that its preference

> is for a uniform national system for the regulation of personal information privacy, which incorporates specific requirements relating to the regulation of health information privacy, rather than a separate code for the regulation of health privacy. Failing this, our preference is for all jurisdictions to adopt and maintain the draft *National Health Privacy Code* for application across the public and private sectors.[88]

---

83 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.

84 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

85 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

86 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

87 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Health and Community Services Complaints Commission (South Australia), *Submission PR 207,* 23 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; South Australian Government Department of Health, *Consultation PC 113*, Adelaide, 2 March 2007; Australasian Compliance Institute, *Consultation PC 53*, Sydney, 17 January 2007; B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

88 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

56.69 The OPC expressed the view that:

> Health privacy regulation could be enhanced by building upon existing provisions, without the necessity of an additional instrument or an entirely new set of principles.
>
> The Office understands that other stakeholders may hold differing views on this matter and would prefer a separate regulatory instrument specifically for the health sector. The Office submits that a uniform and coherent approach to privacy regulation is best served by incorporating privacy protections into a single body of regulation.
>
> A single body of regulation is also likely to reduce regulatory complexity for those agencies and organisations that handle both health and non-health information. The existence of separate sets of principles may create confusion by requiring agencies and organisations to refer to different instruments, depending on the type of personal information they are handling at any given time.[89]

56.70 In the course of the OPC Review, the OPC considered whether it would be possible to incorporate elements of the draft *National Health Privacy Code* into the NPPs. The OPC stated that

> the resulting principles would be longer and more complex. This option would require the insertion of multiple sub-principles and exceptions to the NPPs to take account of the code.
>
> This approach would run counter to the intent of delivering general, high-level principles for all business and government sectors. For instance, the approach would mean that non-health organisations and agencies would need to deal with a more complex set of privacy principles, where much of the content may not apply to them. This would not improve, and may even increase, regulatory complexity overall.[90]

56.71 In addition, the OPC stated in its submission to this Inquiry:

> The Office notes that in a number of significant areas, particularly concerning the collection, use and disclosure of health information, it is questionable whether the proposed NHPC would be likely to be equivalent to the protections of the NPPs … In addition, in a number of areas, the proposed code seems unwieldy, complex and overly prescriptive and, hence, inconsistent with the established light-touch approach to privacy regulation.[91]

56.72 The Australian Privacy Foundation stated that, while in principle the draft *National Health Privacy Code* could form the basis of more detailed principles for health information:

> One difficulty with the development of a separate code is that it encourages drafters and stakeholders to adjust the information privacy principles more than necessary, creating arbitrary or intricate differences that then create confusion. This is evident in the creation of the Health Records Act in Victoria, which adopts much of the

---

89 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

90 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 70.

91 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

> information privacy principles that appeared in the State's Information Privacy Act but is more prescriptive and creates distinctions that may or may not be significant yet cause confusion. For example, the Health Records Act requires organisations in health privacy principle 1.3 to 'take steps that are reasonable in the circumstances to ensure that the individual is generally aware' about the purposes for which the information is collected. By contrast, information privacy principle 1.3 in the Information Privacy Act requires organisations to 'take reasonable steps to ensure the individual is aware' of the same things.[92]

ALRC's view

56.73 The ALRC recognises that handling health information does raise some unique issues and that these require additional consideration in the development of privacy principles, rules and guidelines. For example, in ALRC 96, the ALRC and AHEC noted:

> The collection of family medical history is an established part of medical practice. When providing a health service, health professionals may need to collect family medical history in order to diagnose a patient's condition accurately ... If this information is not collected the medical care or advice provided to the patient may be compromised.[93]

56.74 The ALRC also acknowledges the investment of time and effort that has gone into developing the draft *National Health Privacy Code* and the level of support the Code has among stakeholders. The ALRC's view is, however, that it is undesirable to have two sets of privacy principles, one set dealing with health information and one set dealing with other personal information.

56.75 In Chapter 11, the ALRC examines the impact of inconsistency and fragmentation in the privacy regime and notes that one cost is less sharing of information in appropriate circumstances. This is a particular problem in the health services context where appropriate sharing of health information between members of treating teams is essential to the wellbeing of health consumers.

56.76 In addition, the Taskforce on Reducing Regulatory Burdens on Business (the Regulatory Taskforce) noted that achieving nationally consistent privacy laws is an important factor in reducing compliance costs for business.[94] The Regulatory Taskforce recommended that the Australian Government ask the Standing Committee of Attorneys-General to endorse national consistency in all privacy-related legislation based on the concept of minimum effective regulation.[95] In its response to *Rethinking Regulation*, the Australian Government stated that:

---

92 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

93 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [21.4].

94 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), [4.151].

95 Ibid, rec 4.47.

> The Australian Government agrees to the recommendation and supports the goal of national consistency in privacy-related legislation. At the April 2006 meeting of the Standing Committee of Attorneys-General, Attorneys-General agreed to establish a working group to advise Ministers on options for improving consistency in privacy regulation, including workplace privacy.[96]

56.77 In the ALRC's view, having one set of principles regulating the handling of health information and another set of principles regulating the handling of other personal information would not reduce compliance costs for business and would not be consistent with the goal of national consistency in privacy legislation. In particular, the provisions of the draft *National Health Privacy Code* are not consistent with the provisions of the *Privacy Act*, or with the proposed UPPs—and having two regimes running side by side would contribute to fragmentation, inconsistency and compliance costs for all stakeholders.

56.78 Health information is handled in a range of contexts, not only the health services context. In the ALRC's view, agencies and organisations that handle health information as well as other personal information should not be required to comply with two sets of principles. There is significant overlap in the basic approach to handling health information in state and territory legislation, the NHPPs and the proposed UPPs. For example, UPP 5 provides that sensitive information, including health information, may only be used for the purpose it was collected or a directly related secondary purpose where the individual would reasonably expect the information to be used in that way. This is consistent with the Victorian HPPs and the NHPPs. The NSW HPPs and the ACT privacy principles only require that the purpose be directly related to the purpose for which it was collected.

56.79 In the ALRC's view, the proposed UPPs provide a suitable basic framework for handling health information. With some health specific additions to the UPPs, a single legislative scheme could work effectively to regulate both health information and other personal information. These additions, including some health specific exceptions to the UPPs and a number of health specific additional privacy principles, are discussed in Chapter 57 and include some of the extra principles and exceptions developed for the purposes of the draft *National Health Privacy Code.*

56.80 The ALRC has considered whether the health specific principles and exceptions should sit within the UPPs or alongside the UPPs. Each approach has advantages and disadvantages. If the additional elements were included in the UPPs, the UPPs would be longer and more complex but agencies and organisations would only have to refer to one source of guidance in handling all personal information, including health information. On balance, however, the ALRC proposes that the additional health

---

96 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

information principles and exceptions to the UPPs be set out in regulations to be called the *Privacy (Health Information) Regulations*. This means that, for those agencies and organisations that do not handle health information, the UPPs are concise and more accessible.

56.81 For those agencies and organisations that do handle health information, the ALRC proposes that the OPC publish a document setting out the UPPs as amended by the *Privacy (Health Information) Regulations*. This document will provide a complete set of privacy principles covering health information, as well as other personal information.

56.82 The other reason that the ALRC proposes that health information-specific principles and exceptions be included in regulations is that health is an area in which the application of the proposed UPPs may need to be modified or clarified from time to time. In 2006, for example, the NPPs were amended to provide for the use and disclosure of genetic information to lessen or prevent a serious threat to the life, health or safety of a genetic relative.[97] This kind of change is more easily achieved through regulation, than by amendment of the UPPs in the principal Act.

56.83 The draft *National Health Privacy Code* contains some material that, in the ALRC's view, should be included in the *Privacy (Health Information) Regulations*; that is, where the proposed UPPs need to be amended in relation to health information. This material is discussed in detail in Chapter 57.

56.84 Much of the material in the draft Code, however, is not of this nature. Chapter 15 examines the differences between principles-based regulation and prescriptive rules-based regulation. Principles-based regulation provides greater flexibility, enabling the regime to respond to new issues as they arise without having to create new rules. Rules-based regulation is less flexible and can impose requirements that are not always appropriate in every situation. The draft Code includes a significant amount of material that is closer in nature to rules than principles, setting out how health information is to be handled in particular situations. For example, the Code includes 17 clauses on access to health information. The ALRC's view is that this level of detail is not necessary for inclusion in high-level principles.

56.85 The proposed 'Access and Correction' principle provides a suggested framework for access to personal information. Much of the detail provided in the draft *National Health Privacy Code* in relation to access—for example, how a right of access may be exercised and in what form health information may be provided—is consistent with this principle and could be included in guidelines issued by the OPC. The guidelines could make clear, for example, that organisations may provide a copy of the health information to the individual or, if the individual agrees, an accurate

97 *Privacy Legislation Amendment Act 2006* (Cth).

summary of the health information.[98] The ALRC proposes that the OPC develop such guidelines in consultation with relevant stakeholders and is of the view that the draft Code would provide a valuable starting point in the development of such guidelines.

Proposal 56–2 Health information should continue to be regulated under the general provisions of the *Privacy Act* and the proposed Unified Privacy Principles (UPPs). Amendments to the proposed UPPs that relate specifically to the handling of health information should be promulgated in regulations under the *Privacy Act*—the *Privacy (Health Information) Regulations*.

Proposal 56–3 The Office of the Privacy Commissioner should publish a document bringing together the proposed UPPs and the amendments set out in the *Privacy (Health Information) Regulations*. This document will contain a complete set of the proposed UPPs as they relate to health information.

Proposal 56–4 The Office of the Privacy Commissioner—in consultation with the Australian Government Department of Health and Ageing and other relevant stakeholders—should develop guidelines on the handling of health information under the *Privacy Act* and the *Privacy (Health Information) Regulations.*

Electronic health information systems

56.86 Traditionally, health information has been collected and stored in paper-based systems, with information about one individual held in a number of disparate locations, such as, in general practitioners' records, hospital records, pathology laboratory records and medical specialists' records. Health information increasingly is collected, stored and transferred in electronic form and health information about large numbers of health consumers is collected into central databases, such as the Medicare database and cancer registers.

56.87 Another important trend is the move to integrate health information systems and to create shared electronic health records. Sharing and linking of health information about particular health consumers has the potential to achieve better health outcomes for consumers by allowing health service providers better access to health information, but have also given rise to privacy concerns.

98 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5, div 1, cl 3(1)(b).

Health*Connect* and NEHTA

56.88 In its submission to the OPC Review, DOHA stated:

> A major focus of work in the e-health area for the Department is on implementing Australia's national electronic health records network, Health*Connect*, designed to overcome the gaps in information flow at the point of clinical care. While there is wide acceptance of the benefits that Health*Connect* can deliver, particularly in the areas of patient safety and quality of care, there is also recognition that there are privacy and security risks that need to be managed to ensure such benefits are realised. Personal health information is sensitive information, and both consumers and providers will need to have trust in how their information is handled within and external to Health*Connect* ahead of participating in this system. In this context, privacy and security issues are consistently identified as a key building block for Health*Connect* among all stakeholders.[99]

56.89 A large number of electronic health information systems are being developed at the local, regional and national levels across Australia. For example, in March 2006 the New South Wales Government announced Health*elink*, an electronic health records system to be piloted in different parts of the state.[100] Health*Connect* South Australia is working on three major e-health initiatives including the development of an electronic planning and referral system for health consumers with chronic disease.[101] Health*Connect* Northern Territory has commenced implementation of a Shared Electronic Health Record Service.[102]

56.90 The Health*Connect* website notes that there are a number of developments currently underway that could be implemented nationally within the next 12 to 18 months; for example:

- e-prescriptions—prescriptions for medication being sent electronically from health care providers to pharmacies;
- e-referrals—referrals or requests being sent electronically from one health care provider to another (for example, from a doctor to a radiologist); and
- hospital discharge summaries—summaries of the treatment provided and the proposed future care plan being sent electronically from hospitals to doctors, specialists or aged care facilities.[103]

---

99 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

100 J Hatzistergos (New South Wales Minister for Health), 'Trial of Electronic Health Records' (Press Release, 23 March 2006).

101 HealthConnect South Australia, *HealthConnect South Australia: Health Information When You Need It* <www.healthconnectsa.org.au/> at 13 July 2007.

102 C Burns (Northern Territory Minister for Health), 'Connecting Health Services Territory-Wide' (Press Release, 1 November 2006).

103 Australian Government Department of Health and Ageing, *HealthConnect: FAQs* <www.healthconnect.gov.au> at 1 August 2007.

56.91 The National E-Health Transition Authority (NEHTA) was established in 2005 to set national standards, specifications and infrastructure requirements for electronically collecting and securely exchanging health information. NEHTA is funded jointly by the Australian, state and territory governments. The NEHTA Board is composed of the chief executive officers of the Australian, state and territory health departments. The aim is to ensure a common national approach, setting the necessary foundations for future electronic health systems across Australia.[104]

56.92 NEHTA is also developing a design for a national approach to Shared Electronic Health Records (SEHRs)—records that will contain selected health information about a health consumer, which can be shared among multiple authorised health service providers. An important precursor to SEHRs is the development of a Unique Healthcare Identifiers (UHIs) scheme for individuals and healthcare providers to ensure that information is attributed to the right patient and the right provider:

> Healthcare requires the constant collection, exchange and transmission of health information. This is usually in the context of information about a single patient being exchanged between multiple healthcare providers. It is critical for patient safety and privacy that this information exchange occurs reliably and securely.
>
> The Council of Australian Governments has committed Australia to a single, national approach to identifying individuals and healthcare providers for the purposes of health communications. This approach, being developed by NEHTA, is known as the Unique Healthcare Identification (UHI) Service.
>
> The UHI Service will involve the allocation, issuing and maintenance of unique identifiers for individuals (known as the Individual Healthcare Identifier or IHI) and healthcare providers (the Healthcare Provider Identifier or HPI).[105]

56.93 Unique identifiers are discussed in detail in Chapter 27. In that chapter the ALRC suggests that the proposed 'Identifiers' principle should apply to both agencies and organisations.

56.94 In December 2006, NEHTA released a *Privacy Blueprint—Unique Healthcare Identifiers*,[106] which discusses how NEHTA proposes to manage the privacy issues arising from the UHI Service. The *Privacy Blueprint* states that the Individual Healthcare Identifier (IHI) will be used only to identify individuals for health care and that individuals will not be required to produce an IHI to receive health care.[107] NEHTA notes that in developing national unique healthcare identifiers it will be necessary to assess Australia's privacy laws:

---

104 National E-Health Transition Authority, *About NEHTA* <www.nehta.gov.au> at 1 August 2007.

105 National E-Health Transition Authority, 'Privacy Blueprint—Unique Healthcare Identifiers Release Notes' (Press Release, 13 December 2006).

106 National E-Health Transition Authority, *Privacy Blueprint—Unique Healthcare Identifiers*, Version 1.0 (2006).

107 National E-Health Transition Authority, 'Privacy Blueprint—Unique Healthcare Identifiers Release Notes' (Press Release, 13 December 2006).

> which contain prohibitions and/or restrictions governing the creation and adoption of unique identifiers. These restrictions aim to prevent function creep of identifiers, discouraging their development as almost universal identifiers.[108]

56.95 NEHTA has expressed the view that legislation supporting the creation of the UHI Service would create greater legal certainty, particularly around the creation and distribution of unique identifiers. Other issues that might be covered in such legislation include governance arrangements and sanctions for misuse of the identifiers.[109]

56.96 A report on feedback to the *Privacy Blueprint—Unique Healthcare Identifiers*, noted that:

> Any unique personal identifier, especially where widely held in the community, raises a significant privacy risk of inappropriate datalinking and data-matching. The OPC noted that it will be important to ensure this risk is mitigated and that such a highly reliable identifier is not usurped for purposes beyond the health system and the clinical care of individuals.
>
> The UHI Service potentially holds a very large database on most, if not all, Australians and foreign residents who obtain healthcare. The OPC considered a unique aspect of the proposal is that access to UHI data will be available to a large number of health sector users, raising the risk of misuse or abuse of the data and access privileges, particularly to locate the home address of an individual for purposes unrelated to healthcare. Accordingly, the OPC welcomed NEHTA's detailed measures contained in the Privacy Blueprint directed at protecting individual privacy.[110]

56.97 The OPC Review recommended that:

> The Australian Government should consider developing specific enabling legislation to underpin any national electronic health records system. The legislation should be consistent with the National Health Privacy Code, but also include enhancing protections for matters such as the voluntariness of the system and limitations upon the uses of people's health records.[111]

Submissions and consultations

56.98 In IP 31, the ALRC asked whether electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*.[112] In its submission, the Western Australian Department of Health noted that:

---

108 National E-Health Transition Authority, *Privacy Blueprint—Unique Healthcare Identifiers*, Version 1.0 (2006), 19.

109 Ibid, 24.

110 National E-Health Transition Authority, *Privacy Blueprint on Unique Healthcare Identifiers: Report on Feedback*, Version 1.0 (2007), 5.

111 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 71.

112 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–5.

> Electronic health information systems pose risks to privacy because of the speed and reach of information transfer. However, they also provide new opportunities to increase individual control and to improve security and the ability to audit access to information. Arguably, the privacy issues with electronic systems are not different in kind from those relating to paper-based systems of information storage and general principles are usually appropriate. However, the principles must be informed by a thorough knowledge of electronic storage and transfer practices.[113]

56.99 The NHMRC expressed the view that:

> Despite these risks, we consider that the achievement of national interoperability is a key goal, which will improve the quality of health care offered to the Australian community. The *Privacy Act* needs to facilitate progress and accommodate change efficiently.[114]

56.100 The Office of the Information Commissioner Northern Territory agreed that privacy principles should be drafted at a high level in order to accommodate the handling of personal information in any form:

> The *Privacy Act* and privacy principles do not, and should not, attempt to prescribe detailed requirements for any particular project. They operate at a higher level. Likewise, a national code would operate at a high level and should be reviewed only infrequently. It would be inappropriate to single out electronic health systems for prescriptive treatment that may prove unable to cope with technological changes that appear in a few years time.[115]

56.101 The Office of the Health Services Commissioner in Victoria stated that the provisions of the *Health Records Act* deal adequately with electronic health information systems.[116]

56.102 In its submission, the OPC specifically considered the proposal to establish SEHRs and expressed the view that such systems 'should be accompanied by specific legislative measures to ensure community confidence that personal health information will be handled privately'.[117] The OPC's view is that such legislation should provide for:

- participation on an 'opt-in' basis;
- the primary uses of data;
- a designated authority and processes for approval of secondary uses of data;

---

113 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.
114 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
115 Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007.
116 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.
117 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

- consent processes; and
- sanctions and complaint mechanisms.

56.103 The OPC also suggested that consideration be given to reform of the *Privacy Act* to address the standards by which an individual's health information may be disclosed to and collected from SEHRs.[118]

56.104 DOHA expressed the view that:

> National e-health systems such as Unique Health Identifiers (UHIs) and the Shared Electronic Health Record (SEHR) will significantly change the way health information is handled in the provision of healthcare services. They will lead to greater aggregation of health information which is more searchable. More information about an individual will be potentially available to many more people. The development of these systems will create new opportunities over time for examining this information for the benefit of the individual concerned and the community as a whole, but also carry the possibility of misuse.
>
> For these systems to realise their potential benefits, there must need to be a high level of public trust and confidence in their operation. Express legislative controls over their operation that provide clarity, certainty and predictability, but sufficient flexibility for growth as these systems evolve, are considered integral to building and maintaining this trust and confidence. Reliance on the interpretation and application of general principles is unlikely to be sufficient.
>
> Any legislation must clearly define the purposes for, and the permitted uses of, UHIs and the SEHR. The provisions needed to support the operation and management of key national e-health systems such as UHIs and SEHR services, as these develop, may include:
>
> - the establishment of a standing governance body or bodies to oversight the management and operation of specified e-health systems;
> - who has control over the information collected and how this will be exercised;
> - eligibility criteria, rights and requirements for participation in specified e-health systems by consumers and providers;
> - limitations on the personal information that may be collected in relation to specified e-health systems;
> - the rights of individuals to exercise control over information held about them and to access and correct this information;
> - restrictions on the use or disclosure of the information collected and any penalties for improper use or disclosure;
> - the rules and decision-making processes governing the secondary use of information;
> - the prohibitions on function creep or the mechanisms to authorise any changes in use;

118 Ibid.

- arrangements for ensuring data quality and security of records containing personal information;
- arrangements for access to records and audit logs by the individual concerned or their authorised representative;
- the remedies for improper access and use, including complaints mechanisms; and
- arrangements for enforcing compliance with the standards for interoperability in the healthcare sector that are proposed to be published by the National E-Health Transition Authority (NEHTA).[119]

56.105 NEHTA submitted that it may be desirable to develop specific legislation to support new initiatives that raise issues that fall outside the ambit of statutory privacy regimes, such as governance issues.[120]

ALRC's view

56.106 In the ALRC's view, the collection of health information into electronic health information systems does not require specific legislative control if the *Privacy Act* is updated and amended as proposed in this Discussion Paper. The collection of health information into electronic records and the use of electronic systems to share health information among health service providers treating an individual do not raise new or unique issues. The proposed UPPs and the *Privacy (Health Information) Regulations* are intended to be technology neutral and would satisfactorily regulate the handling of electronic health information.

56.107 However, the establishment of a national UHI scheme or a national SEHR scheme would require specific enabling legislation. The ALRC recognises the significant potential benefits to healthcare quality and safety that the establishment of such schemes may deliver. The schemes will work effectively, however, only if there is a sufficient degree of public trust and public confidence in the schemes and their administration. Further, national developments of such importance involving the establishment and use of unique identifiers for all Australians and the development of a national approach to SEHRs should be subject to public debate and parliamentary scrutiny.

56.108 The ALRC agrees with NEHTA that enabling legislation should deal with those issues that fall outside existing privacy regulation. Such enabling legislation should nominate or establish an agency or organisation with clear responsibility for managing the systems, including the personal information in the systems. There should be clear lines of accountability. The legislation should set out the permitted and

---

119 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.
120 National E-health Transition Authority, *Submission PR 145,* 29 January 2007.

prohibited uses of UHIs and sanctions for misuse. Moreover, the legislation should make absolutely clear that certain safeguards are fundamental; for example, that it is not necessary to use a UHI to access health care.

56.109 The systems should remain subject to the *Privacy Act* and the proposed UPPs as amended by the proposed *Privacy (Health Information) Regulations*. For example, health information generally should only be collected for inclusion in an SEHR with consent. That information should only be used or disclosed for the purpose it was collected or a directly related secondary purpose where the individual would reasonably expect the agency or organisation to use or disclose the information for that purpose.

56.110 Under the proposed 'Identifiers' principle, it would be necessary to set out in regulations those agencies and organisations allowed to adopt, use and disclose UHIs, and the circumstances in which it was lawful for those agencies and organisations to adopt, use or disclose a UHI.

56.111 Exceptions in the UPPs and the regulations would apply so that, for example, it would be possible to use or disclose an individual's health information held in an SEHR if the agency or organisation reasonably believed that the use or disclosure was necessary to lessen or prevent a serious threat to an individual's life, health or safety or public health or public safety.

56.112 The proposals in Chapter 4 are aimed at achieving national consistency in privacy regulation and, in particular, one set of privacy principles applying across the private sector, and the federal, state and territory public sectors. Any legislation establishing the UHI and SEHR schemes also should apply nationally to ensure consistency between the public and private sectors and across all jurisdictions.

Proposal 56–5 The national Unique Healthcare Identifiers (UHIs) scheme and the national Shared Electronic Health Records (SEHR) scheme should be established under specific enabling legislation. The legislation should address information privacy issues, such as:

(a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

(b) the eligibility criteria, rights and requirements for participation in the UHI scheme and the SEHR scheme by health consumers and health service providers, including consent requirements;

(c) permitted and prohibited uses and linkages of the personal information held in the systems;

(d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and

(e) safeguards in relation to the use of UHIs; for example, that it is not necessary to use a UHI in order to access health services.

Medicare and Pharmaceutical Benefits

56.113 The Australian Government holds extensive electronic health records containing personal information collected in connection with claims under the Pharmaceutical Benefits Program and the Medicare Benefits Program. These databases are subject to specific privacy controls over and above those set out in the *Privacy Act*.

56.114 Section 135AA of the *National Health Act 1953* (Cth)[121] deals specifically with the personal information held in these databases. The section requires the Privacy Commissioner to issue written guidelines covering the storage, use, disclosure and retention of the information.[122] The section applies only to information stored in computer databases—principally those held by Medicare Australia and DOHA—and was introduced to ensure the functional separation of information collected in relation to Medicare claims and information collected in relation to pharmaceutical benefits claims.[123]

56.115 This separation was intended to

> accord with the individual patient's expectation that sensitive health information given in a particular context is used and managed by the recipient in a way that is consistent and in accordance with that context. It gives a practical expression, in the context of information storage systems, to the privacy principle that information should generally only be used for the purpose for which it was collected.[124]

56.116 While the information in the two databases is kept functionally separate, it is possible to disclose the information for research purposes, either with consent from the individuals who are the subject of the information or in accordance with guidelines

---

121 Inserted into the *National Health Act 1953* (Cth) by the *Health Legislation (Pharmaceutical Benefits) Amendment Act 1991* (Cth). In addition, s 27(1)(pa) of the *Privacy Act 1988* (Cth) provides that the issue of guidelines under the *National Health Act* is one of the functions of the Privacy Commissioner.

122 Section 27(1)(pa) of the *Privacy Act 1988* (Cth) provides that one of the functions of the Privacy Commissioner is to issue guidelines under s 135AA of the *National Health Act 1953* (Cth).

123 Commonwealth, *Parliamentary Debates*, House of Representatives, 30 May 1991, 4490 (P Staples—Minister for Aged Family and Health Services).

124 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997), Commissioner's Note on cl 1.1.

issued by the NHMRC under s 95 of the *Privacy Act*. The Western Australian Department of Health (WA) has noted that:

> Under current legislation and guidelines, it is possible to create linkable MBS and PBS datasets that contain common encrypted identifiers with ethics clearance. The [Data Linkage Unit] has created linkage keys for these datasets and for Residential Aged Care data from the Department of Health and Ageing that enable unidentifiable data to be provided to researchers in approved projects. Research projects are strictly regulated and 're-identification' and unauthorized linkages are forbidden.[125]

56.117 The Privacy Commissioner first issued the *Medicare and Pharmaceutical Benefits Program Privacy Guidelines* in 1993 and they were last amended in 2000.[126] The Guidelines are legally binding and any breach is an 'interference with privacy' that may provide the basis for a complaint to the Privacy Commissioner.[127] The Guidelines impose obligations on Australian Government agencies in addition to the IPPs in the *Privacy Act* and the secrecy provisions in the *National Health Act* and the *Health Insurance Act 1973* (Cth).

56.118 The Guidelines require that information collected in connection with the Medicare and Pharmaceutical Benefits Programs be stored separately, and specify the circumstances in which data from the two databases may be linked.[128] They modify or supplement the application of the IPPs in some circumstances. For example, the Guidelines modify the application of IPP 11 in relation to disclosure where there is to be linkage, comparison or combination of records from either of the regulated databases. These variations reflect the special sensitivity attached to linkage or comparison of records from the two databases.[129]

56.119 In November 2004, the Privacy Commissioner announced a major review of the Guidelines,[130] prompted by a number of factors, including: a request from DOHA; suggestions that the personal information covered by the Guidelines could be used more effectively by researchers; and suggestions that community attitudes and expectations regarding the handling of personal information—and in particular sensitive health information—may have changed since the Guidelines were issued.[131]

---

125 Department of Health Western Australia, *Submission PR 139,* 23 January 2006. The use of health information for research is discussed in detail in Ch 58.

126 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997). The guidelines are disallowable instruments under the *Acts Interpretation Act 1901* (Cth). They must be tabled in the Australian Parliament and are then subject to disallowance for a period of 15 sitting days.

127 *Privacy Act 1988* (Cth) s 13(bb); *National Health Act 1953* (Cth) s 135AB.

128 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997), cl 1.

129 Ibid, Commissioner's Note on cl 1.4.

130 K Curtis (Privacy Commissioner), 'Media Statement: 2004 Review of the Medicare and PBS Privacy Guidelines Issued under Section 135AA of the National Health Act 1953' (Press Release, 8 November 2004).

131 Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS Claims Information* (2006), 11.

An issues paper[132] was released and 35 submissions were received in the course of the review. A number of open forums were held in late 2004 and a Consultative Group was established to assist the OPC in considering the issues raised in the review.

56.120 The major issues canvassed in the course of the review were the:

- separation of claims information collected under the Medicare and Pharmaceutical Benefits programs;
- circumstances in which claims information from each program may be linked;
- periods for which claims information may be retained;
- use of claims information for medical and other research purposes;
- handling by DOHA of claims information that does not identify individuals; and
- application of the Guidelines to agencies other than Medicare Australia and DOHA.[133]

56.121 The Privacy Commissioner's final report was released in August 2006 and includes 25 findings.[134] Some of these findings will be reflected in revised Guidelines and some set out the OPC's interpretation of matters relevant to the Guidelines. The final report lists the following as key findings:

- The Guidelines should be amended to permit an individual to consent to the linkage of their own claims information by Medicare Australia for the purpose of providing access to the information.[135]
- The prohibition against storing Medicare and Pharmaceutical Benefits claims information on the same database should apply to all agencies.[136]
- Changes should be made to the periods for which Medicare Australia may retain claims information in linked and unlinked form.[137]
- Some changes are required in the way DOHA may handle claims information.[138]

---

132 Office of the Privacy Commissioner, *Review of the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issues Paper* (2004).
133 Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS Claims Information* (2006), 14.
134 Ibid, 8–10.
135 Ibid, finding 2.
136 Ibid, finding 23.
137 Ibid, findings 6–8.
138 Ibid, findings 14–21.

56.122 In light of this recent comprehensive review, the ALRC does not consider it necessary to conduct another detailed study of the Guidelines.

Submissions and consultations

56.123 In IP 31,[139] the ALRC asked whether the role provided for the Privacy Commissioner under s 135AA of the *National Health Act* is an appropriate and effective one. The OPC has submitted that the role is appropriate.[140] Other stakeholders were also supportive.[141]

56.124 In contrast, the Australian Government Department of Human Services stated:

> There is a separate and fundamental question about whether there is still a requirement for section 135AA itself. The information in the Medicare and Pharmaceutical Benefits Scheme claims databases is subject not only to the *Privacy Act* but also to the secrecy provisions of the legislation administered by Medicare Australia. The appropriate application of the privacy principles and secrecy provisions to that information should provide sufficient protection, and as such there is a question about whether there continues to be a need for a separate regime for the handling of the information in those two databases.[142]

ALRC's view

56.125 Although the ALRC did not receive many submissions on this issue, it would appear that there is a role for the Privacy Commissioner in developing rules for handling personal information in major national databases, particularly where databases rely on the use of 'identifiers' such as the Medicare number.[143] Importantly, the current *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines* vary the application of some of the IPPs, reflecting the special sensitivity attaching to, for example, linkage, comparison or combination of records from the two regulated databases. In these circumstances, it is the ALRC's view that it is appropriate for the Privacy Commissioner to be actively involved.

56.126 In Chapter 44, the ALRC considers the role of the Privacy Commissioner more generally in issuing non-binding guidelines and binding rules and expresses the view that the power to issue guidance is an important part of regulating a principles-based regime such as the *Privacy Act*. The ALRC proposes that where guidelines issued by the Privacy Commissioner are binding they should be renamed 'rules' and that the *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines* issued

---

139 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006) Question 8–6.

140 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

141 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; A Smith, *Submission PR 79,* 2 January 2007.

142 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

143 Identifiers are discussed in detail in Ch 27.

under s 135AA of the *National Health Act* should be renamed the *Medicare and Pharmaceutical Benefits Programs Privacy Rules*.[144]

144 Proposal 44–2.

Part H

Health Services and Research

57. The *Privacy Act* and Health Information

Contents

Introduction	1595
Privacy Act 1988 (Cth)	1595
Definition of 'health information'	1596
Definition of 'health service'	1599
Agencies and organisations	1603
Provision of health services	1606
Consent	1609
Privacy (Health Information) Regulations	1614
Collection of health information	1614
Use and disclosure of health information	1626
Access to health information	1633
Management, funding and monitoring	1643

Introduction

57.1 This chapter examines the way in which the *Privacy Act 1988* (Cth) regulates the handling of health information. The chapter considers relevant definitions, such as the definitions of 'health information' and 'health service', and the additions and exceptions in the privacy principles that relate specifically to health information. The chapter focuses on the use of health information in the health services context, including the provision of health care and the management, funding and monitoring of health services.[1]

Privacy Act 1988 (Cth)

57.2 The Information Privacy Principles (IPPs) in the *Privacy Act* do not distinguish between 'personal information', 'sensitive information' and 'health information'. Public sector agencies are required to deal with health information in the same way they deal with other personal information; that is, in accordance with the IPPs.

57.3 The National Privacy Principles (NPPs) provide a separate regime for 'sensitive information', including 'health information', and also deal specifically with the handling of health information in some circumstances. This regime applies to private

1 Ch 58 focuses on the use of health information in research.

sector organisations, including all organisations that hold health information and provide a health service that might otherwise be exempt from the provisions of the *Privacy Act* under the small business exemption.[2]

57.4 The NPPs require that health information be given a higher level of protection than other personal information. For example, health information generally may only be collected with consent.[3] It may be used or disclosed only for the purpose it was collected or a directly related secondary purpose—and only so long as the health consumer would reasonably expect the information to be used in this way.[4] There is also special provision in the NPPs for the:

- collection, use or disclosure of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety;[5]
- collection of health information for the management, funding or monitoring of a health service;[6]
- collection of health information if necessary to provide a health service to the individual and the information is collected as required or authorised by or under law or in accordance with rules relating to professional confidentiality;[7] and
- disclosure of health information to a person who is responsible for the individual, for example, a member of the individual's family, where the individual is physically or legally unable to consent to disclosure.[8]

Definition of 'health information'

57.5 This section considers some of the key elements of the *Privacy Act* relating specifically to the handling of health information, including relevant definitions and exemptions.

57.6 The *Privacy Act* defines 'health information' as follows:

> (a) information or an opinion about:
>
> (i) the health or a disability (at any time) of an individual; or
>
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or

---

2 *Privacy Act 1988* (Cth) s 6D(4)(b). The need for a single set of Unified Privacy Principles (UPPs) applying to both agencies and organisations is discussed in detail in Part D. The small business exemption is discussed in Ch 35.

3 Ibid sch 3, NPP 10.

4 Ibid sch 3, NPP 2.1(a)(i).

5 Ibid sch 3, NPPs 2.1(d), 10.3(a)(i). Research is discussed in detail in Ch 58.

6 Ibid sch 3, NPP 10.3(a)(iii).

7 Ibid sch 3, NPP 10.2.

8 Ibid sch 3, NPPs 2.4–2.6.

> (iii) a health service provided, or to be provided, to an individual;
>
> that is also personal information; or
>
> (b) other personal information collected to provide, or in providing, a health service; or
>
> (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.[9]

57.7 In *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) considered this definition, as well as the definition of 'sensitive information', and concluded that there were circumstances in which genetic information may not fall within the existing definitions.[10] This might arise where the information is not about health, disability or the provision of a health service—as in the case of parentage or forensic testing—or because it is not about the health or disability of an existing individual—as may sometimes be the case with genetic carrier testing, where the information is primarily about the health of future children.[11] On this basis, ALRC 96 recommended that:

> The Commonwealth should amend s 6 of the *Privacy Act 1988* (Cth) (*Privacy Act*) to define 'health information' to include genetic information about an individual in a form which is or could be predictive of the health of the individual or any of his or her genetic relatives.[12]
>
> The Commonwealth should amend s 6 of the *Privacy Act* to define 'sensitive information' to include human genetic test information.[13]

57.8 In September 2006, the *Privacy Legislation Amendment Act 2006* (Cth) was passed. The Act amends the definitions of 'health information' and 'sensitive information' in line with the ALRC and AHEC's recommendations. The amending Act provides that the following paragraph be added to the definition of 'health information':

> (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.[14]

57.9 The definition of 'health information' in the draft *National Health Privacy Code* includes a similar list of elements to the *Privacy Act* definition. The major difference in

---

9 Ibid s 6.

10 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

11 Ibid, [7.75].

12 Ibid, Rec 7–4.

13 Ibid, Rec 7–5.

14 *Privacy Legislation Amendment Act 2006* (Cth) sch 2 cl 2.

the draft Code definition is that it expressly includes information or opinion about 'the physical, mental or psychological health (at any time), of an individual'.[15]

57.10 The definitions of 'health information' in the New South Wales *Health Records and Information Privacy Act*, the Victorian *Health Records Act* and the Northern Territory *Information Act*[16] contain similar elements. The ACT *Health Records (Privacy and Access) Act* defines 'personal health information' more simply as follows:

> any personal information, whether or not recorded in a health record—
>
> (a) relating to the health, an illness or a disability of the consumer; or
>
> (b) collected by a health provider in relation to the health, an illness or a disability of the consumer.[17]

57.11 In the Issues Paper, *Review of Privacy* (IP 31) the ALRC asked whether the definition of 'health information' in the draft *National Health Privacy Code* was appropriate and effective and whether that definition should be adopted into the *Privacy Act*.[18]

Submissions and consultations

57.12 In its submission to the Inquiry, the Australian Government Department of Health and Ageing (DOHA) expressed support for the current definition in the *Privacy Act.* DOHA noted that the dictionary definition of health includes health of body and mind.[19] The *Macquarie Dictionary* defines 'health' as 'soundness of body; freedom from disease or ailment' or 'the general condition of the body or mind with reference to soundness and vigour'.[20] DOHA was of the view that the words 'physical, mental or psychological' included in draft *National Health Privacy Code*, were unnecessary.

57.13 The Office of the Privacy Commissioner (OPC) expressed the view that:

> The proposed NHPC expressly includes 'mental and psychological health' as categories of 'health information', though the existing definition of the *Privacy Act* would already appear to comfortably allow for such an interpretation. In the Office's view, a common sense interpretation of health information would include information relating to mental health.[21]

---

15 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4, cl 1.

16 *Health Records and Information Privacy Act 2002* (NSW) s 6; *Health Records Act 2001* (Vic) s 3; *Information Act 2002* (NT) s 4.

17 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary.

18 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–7.

19 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

20 *Macquarie Dictionary* (online ed, 2005).

21 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

57.14 The NHMRC, however, stated in its submission that:

> The NHMRC is concerned to ensure that the definitions of 'health information' and 'health service' in the *Privacy Act* reflect contemporary and evolving concepts of health and wellbeing.
>
> While many stakeholders would consider that the term 'health' encompasses physical, mental and psychological elements, others draw a distinction between physical 'health' and mental/psychological 'wellbeing'. For clarity, therefore, we support incorporation in the *Privacy Act* of the more expansive definition included in the draft *National Health Privacy Code*.[22]

57.15 A number of other stakeholders also expressed support for the definition in the draft *National Health Privacy Code*.[23]

ALRC's view

57.16 The ALRC acknowledges that the dictionary definition of the term 'health' is broad enough to cover mental and psychological health as well as physical health. The ALRC notes, however, the NHMRC's comment that a distinction is sometimes drawn between physical health and mental or psychological health. The ALRC's view is that the *Privacy Act* should be clear on this point, especially given the sensitivity of personal information about mental or psychological health. It is preferable to clarify the point by amendment than to wait for the issue to arise in the context of a complaint.

Proposal 57–1 The definition of 'health information' in the *Privacy Act* should be amended to make express reference to information or an opinion about the *physical, mental or psychological* health or disability of an individual.

Definition of 'health service'

57.17 Another definition that is central to the way health information is handled under the *Privacy Act* is the definition of a 'health service'. The term is an integral part of the definition of 'health information' and is also used to limit the scope of the small business exemption, discussed below. The Act defines a 'health service' as follows:

> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
>
> (i) to assess, record, maintain or improve the individual's health; or
>
> (ii) to diagnose the individual's illness or disability; or

22 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

23 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

> (iii) to treat the individual's illness or disability or suspected illness or disability; or
>
> (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.[24]

57.18 The definition of 'health service' in the draft *National Health Privacy Code* has a number of differences, including express references to injuries, disability support services, palliative care services, and aged care services. The draft Code definition is as follows:

> 'health service' means—
>
> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual service provider or the organisation performing it—
>
> (i) to assess, maintain or improve the individual's health; or
>
> (ii) to diagnose the individual's illness, injury or disability; or
>
> (iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or
>
> (b) a disability service, palliative care service or aged care service; or
>
> (c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist—
>
> but does not include a health service, or a class of health service, that is prescribed as an exempt health service or to the extent that it is prescribed as an exempt health service.

57.19 The definition in the Victorian *Health Records Act* is very similar to the definition in the draft Code.[25] The definitions in the ACT health records legislation and the Northern Territory *Information Act* have many of the same elements.[26] The New South Wales legislation, however, takes a different approach, setting out a non-exhaustive list of the services covered—such as medical, hospital and nursing services, dental services and mental health services—rather than describing them in more general terms.[27]

57.20 In IP 31 the ALRC asked whether the definition of 'health service' in the draft *National Health Privacy Code* was appropriate and effective and whether that definition should be adopted into the *Privacy Act*.[28]

---

24 *Privacy Act 1988* (Cth) s 6.
25 *Health Records Act 2001* (Vic) s 3.
26 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary; *Information Act 2002* (NT) s 4.
27 *Health Records and Information Privacy Act 2002* (NSW) s 4.
28 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–7.

Submissions and consultations

57.21 There was some support expressed in submissions for the definition of 'health service' in the draft *National Health Privacy Code*.[29] The NHMRC stated that:

> We are aware also that there is some debate in the Aged Care sector about whether residential aged care is a health service or a social/accommodation service. We support, therefore, the inclusion of a more expansive definition of 'health service' in the *Privacy Act*, incorporating reference to 'disability services', 'palliative care services', 'aged care services' and 'injury' explicitly, thereby avoiding any potential uncertainty.[30]

57.22 A number of other stakeholders agreed that the definition should be amended to cover the services that people with a disability, and those in palliative and residential aged care might use. These services provide care, supervision and assistance with daily life, rather than treatment.[31]

57.23 The Office of the Health Services Commissioner in Victoria expressed the view that:

> Organisations providing a broad range of services intended to benefit the health and well-being of individuals, should be subject to the same privacy standards. As an example, HSC has received health privacy complaints concerning alternative therapists, which are included in the definition of health service under the *Health Records Act* and the *National Code*. The problem with the New South Wales approach is that a non-exhaustive definition that focuses on conventional medical and health services may be interpreted to exclude some alternative therapists, which might leave the public vulnerable.[32]

57.24 The OPC raised a number of concerns with the definition of 'health service' in the draft *National Health Privacy Code*, including the fact that the definition does not refer to 'recording' an individual's health information. The draft Code definition also relies exclusively on the understanding of the health service provider as to whether or not a particular activity is intended or claimed to have health benefits. In contrast, the *Privacy Act* allows this to be judged from the perspective of the health service provider or the health consumer. The OPC did, however, express support for one element of the definition:

> The Office also notes that the word 'injury' is added in addition to illness and disability in (a)(ii) and (iii) of the proposed NHPC definition. The nature of an injury

---

29 Health and Community Services Complaints Commission (South Australia), *Submission PR 207,* 23 February 2007; Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

30 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

31 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007; Australian Institute of Health and Welfare, *Submission PR 170,* 5 February 2007.

32 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

> appears to be distinct from the inherent properties of an illness or a disability, and as such, the inclusion of this word may increase the clarity of the definition.[33]

ALRC's view

57.25 The ALRC agrees with stakeholders that the definition of 'health service' in the *Privacy Act* should be extended to cover disability services, palliative care services and aged care services. These services do not fall comfortably within the existing definition of 'health services'. They are, however, aimed at providing physical, mental and psychological care and support to individuals and often require the collection, use and disclosure of significant amounts of health information. The ALRC also agrees that an 'injury' is distinct from an 'illness' or a 'disability' and that the term should be expressly included in the definition of 'health service'.

57.26 It is unclear why the term 'record' is not included in the definition of 'health service' in the draft *National Health Privacy Code*. The ALRC's view is that it should remain in the definition in the *Privacy Act*. Some health monitoring may simply involve the recording of health information—for example, the recording of blood pressure, height and weight over time—with no further action taken in relation to the information unless a change occurs or the information indicates a problem.

57.27 The OPC noted that the definition of 'health service' in the draft *National Health Privacy Code* 'appears to remove the role of the individual's understanding and interpretation of whether or not they believed that a health service was being provided to them'. The ALRC did not receive any submissions indicating problems with the current approach in the *Privacy Act* and is not proposing a change at this time.

Proposal 57–2 The *Privacy Act* should be amended to define a 'health service' as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, record, maintain or improve the individual's health;

  (ii) diagnose the individual's illness, injury or disability; or

  (iii) treat the individual's illness, injury or disability or suspected illness, injury or disability; or

(b) a disability service, palliative care service or aged care service; or

33 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Agencies and organisations

57.28 Broadly speaking, Australian Government agencies are required to handle health information in accordance with the IPPs. Private sector organisations are required to handle health information in accordance with the NPPs. There are a number of significant exemptions in the *Privacy Act*, however, that mean that some agencies and organisations holding health information may not be subject to the Act in relation to that information.

57.29 Perhaps the most significant exemption in the context of health information is for small business operators. Section 6D of the *Privacy Act* defines a small business as one that has an annual turnover of $3 million or less in the previous financial year.[34] Small businesses operators that pose a higher risk to privacy have been brought back into the regime. In particular, small businesses are required to comply with the NPPs if they:

- provide a health service and hold health information, except where the information is held in an employee record;
- disclose personal information for a benefit, service or advantage; or
- provide a benefit, service or advantage to collect personal information.[35]

57.30 Small businesses that hold health information and provide a health service are, therefore, bound by the NPPs. This leaves open the possibility, however, that small businesses that hold health information but do not provide health services, do not pay to collect the information and are not paid to disclose the information—for example, health data registers that store health information for research purposes—may not be required to comply with the Act.

57.31 This possibility was considered in ALRC 96 in relation to genetic information. The ALRC and AHEC concluded that: (a) small businesses that hold genetic information should be subject to the provisions of the *Privacy Act*, whether or not they provide a health service; and (b) there was sufficient doubt about the coverage of

---

34 Ch 35 examines the small business exemption in detail.

35 *Privacy Act 1988* (Cth) s 6D(4). Note that s 6D(7)–(8) of the *Privacy Act* provides that small businesses trading in personal information may not be required to comply with the NPPs if they have the consent of the individuals concerned or if the collection or disclosure of personal information is required or authorised by law.

Privacy Act to justify amending the Act to make it clear that all small businesses that hold genetic information are subject to its provisions.[36]

57.32 The Australian Government did not support this recommendation. The Government considered that the existing provisions provided sufficient protection for the privacy of genetic information held by small businesses, while at the same time ensuring that small businesses were not burdened unfairly by the costs and processes of complying with privacy legislation.[37]

57.33 The draft *National Health Privacy Code*, by way of contrast, is expressed to apply to 'every organisation that is a health service provider or collects, holds or uses health information'.[38] The Victorian *Health Records Act* also applies to organisations that are health service providers or collect, hold or use health information.[39] The Act does not exempt small business operators. On the other hand, the New South Wales *Health Records and Information Privacy Act* exempts small business operators by reference to the *Privacy Act.*[40]

57.34 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act.[41]

Submissions and consultations

57.35 In its submission DOHA noted that:

> It is considered that given its characteristics and sensitivities, individuals need reassurance that their health information will be handled appropriately by whoever holds it. Any misuse will heighten concerns about disclosing this kind of information, and unwillingness to disclose this information in a healthcare setting could result in detriment to the individual concerned or to the community as a whole.[42]

57.36 DOHA expressed the view that the handling of health information should be subject to appropriate privacy regulation across both the public and private sectors, although noting the need for some exemptions for agencies and organisations such as the courts. Other stakeholders agreed that appropriate privacy regulation should apply

---

36 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 7–7.

37 Australian Government Attorney-General's Department, *Government Response to Australian Law Reform Commission and Australian Health Ethics Committee Report: Essentially Yours: The Protection of Human Genetic Information in Australia* (2005) <www.ag.gov.au> at 30 July 2007, 8.

38 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 2 div 1 cl 1.

39 *Health Records Act 2001* (Vic) s 11.

40 *Health Records and Information Privacy Act 2002* (NSW) s 4.

41 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–8.

42 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

in both the public and private sectors and regardless of the size of the business involved.[43]

57.37 In its submission, the NHMRC stated that:

> The NHMRC cannot identify any relevant policy rationale for excluding the majority of small businesses from compliance with the *Privacy Act*. We consider that it is vitally important that the protections currently provided for health information apply to all agencies and organisations that handle health information (including genetic information) and to all agencies and organisations that handle genetic information that is not health information.[44]

ALRC's view

57.38 Part E examines the policy basis for each of the exemptions from the *Privacy Act* and makes proposals for change where necessary. In Chapter 35, the ALRC proposes the removal from the *Privacy Act* of the small business exemption. The ALRC is not convinced that an exemption for small business is either necessary or justifiable. The fact that comparable overseas jurisdictions—including the United Kingdom, Canada and New Zealand—do not have an exemption for small business is a relevant consideration. In addition, the removal of the exemption may assist in achieving adequacy under the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) and facilitate trade with EU organisations. Removal of this exemption will mean that it is no longer necessary to bring small businesses that handle health information back into the regime.

57.39 In Chapter 36, the ALRC further proposes the removal from the Act of the employee records exemption. This will extend privacy protections to health information held in private sector employee records for the first time.

57.40 The ALRC's view is that, once implemented, the proposals in Parts D and E will ensure that personal information—and, in particular, health information—will receive appropriate protection in the Australian Government public sector and the private sector. The proposals in Chapter 4, aimed at achieving national consistency, will extend this protection into state and territory public sectors. These proposals in

---

43 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Health Informatics Society of Australia, *Submission PR 196,* 16 January 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Royal Women's Hospital Melbourne, *Submission PR 108,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; W Caelli, *Submission PR 99,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006; A Smith, *Submission PR 79,* 2 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

44 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

combination will mean that the handling of health information is regulated consistently and appropriately throughout Australia.

Provision of health services

57.41 The following section deals with the impact of the *Privacy Act* on the provision of health services to health consumers. It was suggested in consultations that the *Privacy Act* impeded the provision of health services to consumers by, for example, interfering with the appropriate sharing of an individual's health information between members of the team of health professionals treating the individual.[45] This may be a result of problems with the *Privacy Act*, which are discussed below in relation to particular privacy principles, or it may be for other reasons. For example, there may be a chilling effect on the sharing of information based on a misunderstanding of, or an overly cautious approach to, the Act or the privacy principles rather than a correct application of the Act and principles.

57.42 In its submission to the Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act* (the OPC Review),[46] the NHMRC stated that:

> The NHMRC considers that the application and/or interpretation of the *Privacy Act* is impairing the quality, effectiveness and timeliness of management of health information. In their efforts to ensure compliance with the law, health care professionals and administrators are experiencing considerable difficulty in developing and implementing practical policies that do not 'over-interpret' their obligations and do not impair the legitimate flow of information between providers for patient care purposes.
>
> The NHMRC also considers that the overall public interest and the interests of the majority of individual patients are served by the efficient transfer of all necessary clinical information between health care providers for the purposes of the current care of an individual patient. There is, in fact, considerable potential for individual harm as a result of a privacy regime which results in individual health care providers being uncertain about their legal obligations, afraid of breaking the law by transferring health information without explicit consent, and implementing ineffective and inefficient procedures in their efforts to comply with the law.[47]

57.43 The OPC Review recommended the development of further guidance in relation to the use and disclosure of health information in the health services context under the NPPs.[48]

---

45 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006.

46 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).

47 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

48 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 77, 78.

Submissions and consultations

57.44 In its submission to the Inquiry, DOHA stated that:

> It is not possible to point to specific evidence of incidents where the present regulatory environment for health information has impeded the provision of health service delivery. Anecdotally, in handling enquiries on privacy matters Departmental officers are aware of instances where callers have complained about a request for information being refused 'because of the Privacy Act'. In discussions with private medical practitioners, frustration has been expressed about not being able to easily obtain information from a public hospital about a recent admission of one of their patients for the purpose of treatment. These kinds of responses and perceptions often result from a misunderstanding of the privacy regulation, something that is not helped by the inconsistencies, complexities and confusion that results from the present regulatory environment.[49]

57.45 This is consistent with comments in other submissions that indicate that the problem is not the content of the privacy principles themselves but a lack of understanding of relevant legislation and principles.[50] The Western Australian Department of Health also suggested that part of the problem lies in changing clinical practice that now involves multiple health service providers from a greater range of institutions in the treatment of one individual. The Department noted the need for communication and education to manage this transition.[51]

57.46 The NHMRC expressed the view that the principles could be made clearer:

> The NHMRC has significant anecdotal evidence and survey responses indicating that disclosure of health information for the purposes of current treatment is being impeded by the privacy regulatory regime. We consider that disclosure of relevant health information for current treatment purposes should be permitted provided there is no indication to the disclosing organisation that such disclosure is or would be unacceptable to the patient; and there are no other circumstances which could reasonably be expected to alert the disclosing organisation that the patient would object to disclosure. We consider that this issue is of sufficient significance to warrant recognition, through a binding determination, legislative or regulatory change, of the circumstances in which disclosure can be made for the purposes of ongoing clinical care.[52]

57.47 The OPC, however, expressed the view that the NPPs are consistent with best practice and professional ethical standards in the health services context. The OPC suggested that the major impediments to appropriate information flow between health service providers was uncertainty created by regulatory complexity and overlapping

---

49 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

50 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; A Smith, *Submission PR 79,* 2 January 2007.

51 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

52 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

and inconsistent legislation regulating the handling of health information in different jurisdictions.[53]

57.48 The Office of the Victorian Health Services Commissioner was of the view that the Health Privacy Principles (HPPs) in the *Health Records Act* were based on good standards of health service delivery and did not cause problems of the type discussed above. The Office suggested that the problem arose from a different source:

> As a result of the introduction of privacy legislation, individuals who believe their privacy has been breached have somewhere to complain, and this makes some health providers more cautious in their dealings with individuals. Some health service providers have interpreted privacy to mean secrecy. The solution is training, resources and support.[54]

ALRC's view

57.49 While there was some evidence in submissions and consultations that the regulation of health information in Australia is causing problems for health service providers, there was very little evidence that the problem lies with the IPPs or NPPs. The problems identified included confusion caused by regulatory complexity and a lack of understanding of some of the principles and how they might apply in the health services context. The ALRC's view is that the proposals in Chapter 4 aimed at achieving national consistency in privacy regulation, in combination with proposals for one set of Unified Privacy Principles (UPPs) and a rationalisation of the exceptions and exemptions in the *Privacy Act*, will go a long way towards resolving the uncertainty and confusion caused by the existing regime.

57.50 As discussed in Chapter 15, a principles-based privacy regime focuses on high-level, broadly stated principles rather than detailed, prescriptive rules. This is intended to shift the regulatory focus from process to outcomes. Principles-based regulation facilitates regulatory flexibility through a statement of general principles that can be applied to new and changing situations. This is considered entirely appropriate and workable in the health services context.

57.51 The proposed UPPs provide that health information generally must be collected with consent, although that consent may be express or implied. Health information may be used or disclosed for the purpose for which it was collected and any other directly related purpose, within the reasonable expectations of the individual health consumer. These principles provide extensive scope for exchange of information among members of treatment teams, while encouraging good communication with health consumers about the collection, use and disclosure of their health information. The principles do not require written consent from the health consumer for every collection, use or disclosure. The principles do not prevent the sharing of health information among the members of a team of health service providers treating a health consumer. There was

---

53 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

54 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

no evidence provided to the Inquiry that these basic principles were inappropriate or unworkable, in practice.

57.52 In addition, there are a number of exceptions to the principles that, while applying broadly to personal information, are relevant to the handling of health information in the health services context. These include the exceptions in the:

- proposed 'Collection' principle, which allows the collection of sensitive information, including health information, without consent where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent; and

- proposed 'Use and Disclosure' principle, which allows the use or disclosure of personal information, including health information, if the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety or to public health or public safety.

57.53 Finally, there are a number of principles and exceptions that apply only to health information. In Chapter 56, the ALRC proposes that these principles and exceptions should sit in the *Privacy (Health Information) Regulations*. Each of these principles and exceptions is considered below.

57.54 The OPC has recommended the development of further guidance in relation to the use and disclosure of health information in the health services context.[55] The ALRC supports this approach. In light of the comments from stakeholders noted above, it seems clear that there is a need for further guidance and training for health service providers to ensure a better understanding of the intent and application of principles-based regulation and the privacy principles. It may also be that this issue requires further focus from providers of education and training in the health services context. The ALRC notes, however, that in a principles-based regime there always will be a need for the exercise of judgement and discretion by agencies and organisations handling health information.

Consent

57.55 Consent is a central concept in the *Privacy Act* and is of particular importance in dealing with health information because of the sensitive nature of that information. Consent provisions allow individual health consumers a measure of control over the collection, use and disclosure of their health information. This contributes to an

55 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), recs 77, 78.

environment in which the autonomy and dignity of the individual are respected, and supports the public interest in health consumers seeking advice and assistance from health service providers when needed, with the assurance that they will be able to maintain appropriate control of their personal information. It is important to note in the context of the *Privacy Act* that the issue under consideration is consent to the handling of health information and not consent to medical treatment.

57.56 The role of consent in the privacy regime generally, including issues such as the definition of consent and the use of 'bundled consent', is considered in detail in Chapter 16. In this chapter the ALRC will consider the role of consent in dealing with health information.

57.57 The OPC *Guidelines on Privacy in the Private Health Sector* (OPC Guidelines) state that the key elements of consent are:

- it must be provided voluntarily;
- the individual must be adequately informed; and
- the individual must have the capacity to understand and communicate their consent.[56]

Consent in the IPPs and the NPPs

57.58 In general terms, both the IPPs and the NPPs attempt to align consent requirements with what health consumers would reasonably expect in relation to the handling of their health information.

57.59 Consent is generally required when collecting health information under the NPPs.[57] Consent is not, however, required when collecting health information under the IPPs.[58] Consent is not required for use under the NPPs or the IPPs if health information is used for the purpose for which it was collected or any other directly related purpose and, in the case of the NPPs, individuals would reasonably expect the organisation to use health information in that way.[59]

57.60 Consent is not required for disclosure under the IPPs if the individual was reasonably likely to have been aware that such disclosures are usually made.[60] Consent is not required for disclosure under the NPPs if the information is disclosed for the

---

56 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.2.
57 *Privacy Act 1988* (Cth) sch 3, NPP 10.1.
58 Ibid s 14.
59 Ibid s 14, IPP 10.1; sch 3, NPP 2.1.
60 Ibid s 14, IPP 11.1.

purpose for which it was collected or a directly related purpose and individuals would reasonably expect the organisation to disclose health information in that way.[61]

57.61 There are a number of exceptions to these general rules. For example, health information may be used without consent under both the IPPs and the NPPs where the use is: necessary to lessen or prevent a serious and imminent threat to an individual's life or health;[62] required or authorised by law;[63] or reasonably necessary to enforce the criminal law.[64]

57.62 There is also a regime established to allow health information to be used without consent for research in some circumstances, with the approval of a Human Research Ethics Committee (HREC). This regime is discussed in detail in Chapter 58.

Express and implied consent

57.63 'Consent' is defined in the *Privacy Act* as 'express or implied consent'.[65] Express consent 'refers to consent that is clearly and unmistakably stated'.[66] It may be stated orally, in writing, electronically or in any other form, so long as the consent is clearly communicated. Implied consent also requires communication and understanding between health service providers and health consumers. The OPC has stated that:

> If the discussion has provided the individual with an understanding about how their health information may be used, then it would be reasonable for the health service provider to rely on implied consent.[67]

Specific and general consent

57.64 Consent runs along a spectrum from the very specific to the very general. In some cases consent is sought to a wide range of uses and disclosures of personal information without giving individuals an opportunity to distinguish between those uses and disclosures to which they consent and those to which they do not. This is a particular problem where some of the uses and disclosures bundled together do not relate to the primary purpose of collection. This is referred to as 'bundled consent' and is discussed in Chapter 16.

57.65 In relation to sensitive information, such as health information, it may be reasonable to seek consent to a range of things at the same time—for example, collection into a health record maintained by the health service provider that will be

---

61 Ibid sch 3, NPP 2.1.
62 Ibid s 14, IPP 10.1(b); sch 3, NPP 2.1(e).
63 Ibid s 14, IPP 10.1(c); sch 3, NPP 2.1(g).
64 Ibid s 14, IPP 10.1(d); sch 3, NPP 2.1(h).
65 Ibid s 6.
66 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.3.
67 Ibid, Guideline A5.3.

retained for some period into the future; disclosure to and use by a pathology laboratory for testing purposes; and disclosure to a medical specialist for expert advice. Consent, however, should not be so general as to undermine the requirements that it be voluntary and adequately informed.

Capacity

57.66 Significant issues arise when individuals do not have the capacity to understand and communicate their consent to the way in which their health information is handled. For example, an adult's decision-making capacity may be impaired temporarily or permanently by injury, illness or disability. This issue is discussed in detail in Chapter 61. Children and young people may have limited capacity to understand and consent. This issue is discussed in Chapter 60.

57.67 The draft *National Health Privacy Code* provides detailed provisions in relation to the powers of an 'authorised representative'. These provisions include powers to consent to collection, use and disclosure of health information on behalf of an individual who is incapable of giving consent, as well as powers to access and correct health information.[68]

57.68 In IP 31, the ALRC asked whether the *Privacy Act* provides an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent.[69] The ALRC also asked whether there are any other issues relating to consent to deal with health information in the health services context that the ALRC should consider.[70]

Submissions and consultations

57.69 In its submission, DOHA stated that:

> Where the individual lacks capacity, it should be permissible for a person who is authorised under general law to make decisions on behalf of the individual, such as a parent, legal guardian or a person with an enduring power of attorney, to give consent, or to exercise rights of access or correction.[71]

57.70 A number of stakeholders expressed the view that detailed guidance was required in this area.[72] There was some support for the approach adopted in the draft *National Health Privacy Code.*[73] The National E-Health Transition Authority (NEHTA) commented, however, that although the draft Code included provision for an

---

68 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4 cl 4.

69 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–11.

70 Ibid, Question 8–12.

71 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

72 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.

73 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

'authorised representative' to make decisions on behalf of an individual, the Code did not allow for less formal arrangements. NEHTA's view was that it was important to allow sufficient flexibility for alternative decision making in the health services context.[74]

ALRC's view

57.71 Chapter 16 discusses the concept of consent in detail, including what amounts to valid consent and the problem of 'bundled consent'. In that chapter the ALRC proposes that the OPC provide further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act* in specific contexts, and on when it is or is not appropriate to use the mechanism of 'bundled consent'.[75]

57.72 Chapter 61 considers in detail the issue of adults with a decision-making disability. In that chapter the ALRC proposes adopting the concept of 'authorised representative' from the draft *National Health Privacy Code* into the *Privacy Act* with some amendments. Where an individual is incapable of giving consent, making a request or exercising a right under the Act, an 'authorised representative' may give the consent, make the request or exercise the right on behalf of the individual. An individual is considered incapable of giving consent under the Act if, despite the provision of reasonable assistance by another person, he or she is incapable of understanding the general nature and effect of giving the consent or is incapable of communicating consent or refusal to consent.[76]

57.73 The ALRC proposes that the term 'authorised representative' be defined as: a guardian appointed under law; a guardian appointed under an enduring guardianship appointment; an attorney under an enduring power of attorney; a person who has parental responsibility for the individual if the individual is under the age of 18; or a person otherwise empowered under law to perform any functions or duties as agent or in the best interests of the individual.[77]

57.74 The ALRC's view is that these proposed provisions, in combination with the proposed UPPs, will provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent. In emergency situations, paragraph 2.6(c) of the proposed 'Collection' principle—which allows the collection of health information without consent where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual—and paragraph 5.1(c) of the proposed 'Use and Disclosure' principle—which allows the use or disclosure of health information where necessary to lessen or

---

74 National E-health Transition Authority, *Submission PR 145,* 29 January 2007.
75 Proposal 16–1.
76 Proposal 16–1.
77 Proposal 61–2.

prevent a serious threat to an individual's life, health or safety or to public health or public safety—will operate. In other circumstances, an 'authorised representative' may act on behalf of the individual.

Privacy (Health Information) Regulations

57.75 In this section the ALRC considers existing and proposed privacy principles and exceptions to the privacy principles that deal specifically with the handling of health information. As discussed in Chapter 56, the ALRC's view is that these principles and exceptions should be set out in *Privacy (Health Information) Regulations*.[78]

57.76 The ALRC's view is that, for those agencies and organisations that do not handle health information, it is important to keep the UPPs shorter and more accessible. For those agencies and organisations that do handle health information, the ALRC proposes that the OPC publish a separate document setting out the UPPs as amended by the *Privacy (Health Information) Regulations*. This document will provide a complete set of privacy principles covering health information, as well as other personal information.

Collection of health information

Collection of family medical history information by health service providers

57.77 NPP 10.1 provides that, subject to a number of exceptions, an organisation must not collect sensitive information without consent. This requirement is also included in the 'Collection' principle in the proposed UPPs.[79] On 21 December 2001, the Privacy Commissioner made two Temporary Public Interest Determinations (TPIDs) in response to concerns that the long standing and accepted practice of collecting health information about third parties—for example, family members—without their consent for inclusion in the social and medical histories of health consumers may breach the NPPs.

57.78 The TPIDs were given effect for up to 12 months, to permit the Privacy Commissioner to conduct consultations on the issue. Over 60 submissions were received during the consultation period, and a conference was held in August 2002 to consider a draft determination.[80] The Privacy Commissioner formed the view that the collection of health information about third parties without consent in the course of delivering a health service was a breach of NPP 10.1, and that the act or practice should nevertheless be allowed to continue. In the Privacy Commissioner's view, the public interest in its continuation substantially outweighed the public interest in adhering to NPP 10.1:

---

78 Proposal 56–2.

79 The IPPs do not require that agencies have consent before collecting health information and so the same issue did not arise.

80 *Privacy Act 1988* (Cth) s 76 provides for a conference to be held to consider a draft determination on the Privacy Commissioner's initiative.

> The collection of family, social and medical history information is a critical part of providing assessment, diagnosis and treatment to individuals. The Commissioner acknowledged that obtaining the consent of third parties to collect their information, and notifying those individuals about these collections, would be impractical, inefficient and detrimental to the provision of quality health outcomes.[81]

57.79 In October 2002, the Privacy Commissioner made two public interest determinations (PIDs)—PID 9 in relation to the particular health service provider that made the original application and PID 9A in relation to health service providers generally—to replace the TPIDs. PIDs 9 and 9A were tabled in the Australian Parliament and took effect on 11 December 2002 for a period of up to five years. Under PIDs 9 and 9A health service providers may collect health information from health consumers about third parties without consent when both of the following circumstances are met, the:

- collection of the third party's information into a health consumer's social, family or medical history is necessary to enable health service providers to provide a health service directly to the consumer; and

- third party's information is relevant to the family, social or medical history of that consumer.[82]

57.80 A review of the PIDs is to take place by October 2007, or sooner, if the Commissioner becomes aware of any matter incidental to or affecting the performance or operation of the PIDs.

57.81 In the course of the OPC Review, a number of issues were raised in relation to PIDs 9 and 9A. The first was whether the effect of the PIDs should be made permanent by an amendment to the *Privacy Act*. A number of submissions to the OPC Review commented on the effectiveness and importance of PIDs 9 and 9A and expressed support for such an amendment.[83]

57.82 National Health Privacy Principle 1 (NHPP 1) of the draft *National Health Privacy Code* specifically provides for the collection of health information without consent where

---

81 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 274.

82 Privacy Commissioner, *Public Interest Determination 9*, effective 11 December 2002; Privacy Commissioner, *Public Interest Determination 9A*, effective 11 December 2002.

83 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004; Mental Health Privacy Coalition, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

the information is a family medical history, social medical history or other relevant information about an individual, that is collected for the purpose of providing a person (including the individual) with a health service, and is collected by a health service provider:

(i) from the person who is to receive that service; or

(ii) from a relative or carer of the individual;[84] or

(iii) in any other situation, in accordance with any guidelines issued for the purposes of this paragraph.[85]

Submissions and consultations

57.83 A number of stakeholders, including the OPC, expressed support for amending the *Privacy Act* to give statutory effect to PIDs 9 and 9A.[86] The OPC noted that the PIDs are due to expire on 11 December 2007 and that no submissions to the OPC Review were critical of the content of the PIDs. The OPC suggested, however, that consideration might be given to limiting the provision to exclude genetic information and information in electronic health records, given the potential detail in such sources.[87]

57.84 In its submission, the OPC expressed a preference for the wording of the PIDs over the wording of NHPP 1 of the draft *National Health Privacy Code* on the basis that the health sector has been working with the wording of the PIDs for a number of years. The OPC suggested, however, that there may be merit in including the provision from the draft Code allowing collection of health information about third parties from 'a relative or carer of the individual'.[88] A number of other stakeholders expressed a preference for the wording in NHPP 1 of the draft Code.[89]

57.85 The NHMRC suggested that an amendment was also needed to the notification requirements in NPP 1.5. NPP 1.5 requires that, where an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in

---

84 This paragraph would apply, for example, where the individual was a child or an adult with a decision-making disability. Handling the health information of children, young people and adults with a decision-making disability is discussed further in Part I of this Discussion Paper.

85 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 1.1(i).

86 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

87 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

88 Ibid.

89 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; A Smith, *Submission PR 79,* 2 January 2007.

NPP 1.3, such as the identity of the organisation and the purpose for which the information was collected. The NHMRC submitted that:

> NPP 1 should be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is:
>
> - notified of the fact that personal information about them has been collected from a third party; and/or
> - made aware of the specified matters relating to the collection and/or disclosure of that personal information.[90]

57.86 The NHMRC noted that the Privacy Commissioner had not included an exemption from the notification requirements in PIDs 9 and 9A. Instead, the Privacy Commissioner confirmed that, in the normal course of events, a health service provider will not be required to notify third parties that their health information has been collected for inclusion in the family, social or medical history of another individual.

> The NHMRC submits that it would be unreasonable to require notification in such circumstances. While notification in any individual case may be feasible, notification in relation to the vast number of patient encounters at which such information is collected would be administratively burdensome and practically impossible in many cases. In addition, a notification requirement would be likely, in many circumstances, to impair the provision by consumers to their health care providers of sensitive information about family members, which may be vital to their own health care.[91]

ALRC's view

57.87 The ALRC's view is that PIDs 9 and 9A should be given statutory effect by being promulgated in the *Privacy (Health Information) Regulations*. The collection of health information about family members and others is routine practice and essential to provide appropriate health care to individuals.

57.88 The proposed regulation should not expressly exclude genetic information or information in electronic health records. Genetic information, because of its familial nature, is particularly important in family medical histories. The proposed regulation should, however, be limited to collection of health information about third parties from the individual health consumer or a person who is 'responsible for' the individual, as discussed further below. This will limit the amount and type of health information collected about third parties.

57.89 A regulation along these lines would not, for example, allow health service providers to collect health information from third party genetic samples. In addition, an individual health consumer will not generally have access to comprehensive genetic or electronic health records about third parties without their consent, and so will not be

---

90 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
91 Ibid.

able to provide these to health care providers without the knowledge and consent of the third party.

57.90 The ALRC agrees that, in general, PIDs 9 and 9A are preferable to NHPP 1. In relation to the collection of third party information from relatives and carers, however, the ALRC's view is that NHPP 1 makes a valuable addition to the PIDs. For example, it may be necessary to collect third party information from parents attending a health service with a child or from a spouse or partner where the health consumer is unconscious. The concept of a 'responsible person' is discussed in detail below but would include a family member, carer or 'authorised representative'. The ALRC proposes, therefore, that a health service provider be able to collect third party information from a health consumer, or a person responsible for the health consumer, where the collection of the third party's information is necessary to enable the health service provider to provide a health service to the consumer and the third party's information is relevant to the health consumer's family, social or medical history.

57.91 The ALRC notes the concerns raised by the NHMRC in relation to the notification requirements in NPP 1.5. The ALRC agrees that it is unreasonable to require health service providers to notify third parties that personal information about them has been collected in the context of taking a family medical history. Under the proposed 'Specific Notification' principle, where an agency or organisation collects personal information from an individual about a third party, the agency or organisation is only required to take reasonable steps to notify the third party in circumstances where a reasonable person would expect to be notified. The ALRC's view is that a reasonable person would not expect to be notified when his or her personal information was collected by a health service provider in these circumstances.

Proposal 57–3 The *Privacy (Health Information) Regulations* should provide that a health service provider may collect health information from a health consumer, or a person responsible for the health consumer, about third parties without consent when:

(a) the collection of the third party's information into a health consumer's social, family or medical history is necessary to enable health service providers to provide a health service directly to the consumer; and

(b) the third party's information is relevant to the family, social or medical history of that consumer.

Collection of family medical history information by insurance companies

57.92 The second issue raised in the OPC Review was the collection of third party health information without consent by insurance companies. In ALRC 96, the ALRC and AHEC noted that:

> Insurance companies routinely collect family medical history information and use it in underwriting. The collection and use is based on the long recognised fact that certain diseases have a hereditary component, and that information about the medical history of family members is relevant in assessing the applicant's risk.[92]

57.93 The public interest issues to be considered in relation to the collection of this information by insurers are not the same as those considered in the development of PID 9 and PID 9A, which focused on collection by health service providers. The ALRC and AHEC expressed the view that it would be appropriate to consider the specific issues that arise in the insurance context in the course of a PID process. The ALRC and AHEC recommended that:

> Insurers should seek a Public Interest Determination under the *Privacy Act 1988* (Cth) in relation to the practice of collecting genetic information from applicants about their genetic relatives for use in underwriting insurance policies in relation to those applicants.[93]

57.94 The OPC Review noted that, to date, the Privacy Commissioner had not considered an application for a PID in these terms[94] and recommended that:

> The Australian Government should consider undertaking consultation on limited exceptions or variations to the collection of family, social and medical history information, particularly with regard to genetic information and the collection practices of the insurance industry.[95]

57.95 In IP 31, the ALRC asked whether the *Privacy Act* should be amended to allow insurance companies to collect health information about third parties without their consent in similar circumstances to those set out in Public Interest Determinations 9 and 9A.[96]

Submissions and consultations

57.96 The Insurance Council of Australia expressed support for amending the *Privacy Act* to allow insurance companies to collect health information about third parties without their consent, noting that, 'in some instances health information of a third party is relevant to the medical history of a claimant and therefore required to properly manage and understand a claim'.[97] The Investment and Financial Services Association

---

92 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.49].

93 Ibid, Rec 28–3.

94 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 276.

95 Ibid, rec 82.

96 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–14.

97 Insurance Council of Australia, *Submission PR 110,* 15 January 2007.

(IFSA) and a number of other stakeholders also expressed support for a specific exception.[98]

57.97 The Office of the Health Services Commissioner in Victoria noted that an amendment would be desirable to ensure that insurance companies are using third party information only for the purpose of processing individual insurance contracts and claims, and in compliance with the *Privacy Act*. The Office submitted that 'clarity is needed in this area, and a working group should be set up to consult with stakeholders to come up with a suitable position on the issue'.[99]

57.98 By contrast, the OPC and other stakeholders did not support an exception to allow insurance companies to collect third party information without consent.[100] The OPC noted that the nature of the interests involved in the provision of health services and the provision of insurance differ considerably. While PIDs 9 and 9A concern the collection of third party information for the preservation of life and health, the collection of such information by insurance companies involves actuarial decision making and loss distribution. The OPC expressed the view that, while important, 'the latter arguably lacks the compelling policy considerations necessary to warrant potentially lessening privacy protections'.[101]

57.99 The OPC noted that the IFSA *Family Medical History Policy* provides a practical solution to compliance with the *Privacy Act*. The Policy states 'insurers will not collect family medical history information in an identifiable format'.[102] The OPC expressed support for this approach, which allows the insurance industry to collect relevant third party health information while complying with the requirements of the *Privacy Act*.

ALRC's view

57.100 The ALRC notes that the insurance industry has not, to date, applied to the Privacy Commissioner for a PID in relation to the collection of family medical history information without consent. IFSA's *Family Medical History Policy* appears to indicate that it is feasible for insurers to collect and use health information about family members that does not identify those family members. If this is so, then amending the *Privacy Act* is unnecessary. If information collected by insurance companies is not 'about an individual whose identity is apparent, or can reasonably be ascertained, from

98 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Investment and Financial Services Association, *Submission PR 122,* 15 January 2007.

99 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

100 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; K Pospisek, *Submission PR 104,* 15 January 2007; I Turnbull, *Submission PR 82,* 12 January 2007.

101 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

102 Investment and Financial Services Association, *Family Medical History Policy: IFSA Standard No 16.00* (2005), [10.2].

the information' it does not fall within the definition of 'personal information' and is not covered by the *Privacy Act.*

57.101 The ALRC notes, however, that the accompanying commentary in the IFSA *Family Medical History Policy* states that 'Family medical history information collected will be done so [sic] on a de-identified basis, that is name and date of birth of the relative will not be collected.'[103] Collecting information without names and date of birth attached may not be sufficient to ensure that information is not 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information'. If, for example, it is apparent from the information collected that the family member is the mother or father of the individual applying for insurance, the individual's identity can reasonably be ascertained from the information. In order to comply with the existing provisions of the *Privacy Act*, insurance companies must ensure that any third party health information they collect without consent is not about an individual whose identity is apparent or can reasonably be ascertained.

57.102 The ALRC is concerned that, although names and date of birth are not collected, family member's identities may be reasonably ascertainable from other information collected. If this is the case, insurance companies are collecting third party health information in breach of the *Privacy Act*. The ALRC is of the view that if this is the case, insurers should seek a PID under the *Privacy Act* in relation to the practice. This is consistent with the relevant recommendation in ALRC 96,[104] discussed above.

Collection of health information as required or authorised by or under law

57.103 As noted above, NPP 10.1 provides in part that an organisation must not collect sensitive information, including health information, without consent except in a number of specified situations. One of those is where 'the collection is required by law'.

57.104 NPP 10.2 provides a further exception to the general rule that health information must not be collected without consent. NPP 10.2 provides:

> Despite subclause 10.1, an organisation may collect health information about an individual if:
>
> (a) the information is necessary to provide a health service to the individual; and
>
> (b) the information is collected:
>
> (i) as required or authorised by or under law (other than this Act); or

103 Ibid, [10.2.1].

104 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 28–3.

> (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

57.105 NPP 10.2 recognises that health service providers may have legal obligations to collect certain health information without consent in the course of providing a health service. The OPC Guidelines note that 'law' includes Commonwealth, state and territory legislation, as well as the common law.[105] State and territory public health Acts, for example, require health service providers to collect and record certain information about health consumers with 'notifiable diseases', such as, tuberculosis, Creutzfeldt-Jakob disease and HIV/AIDS.[106]

57.106 It is unclear, however, why the language in NPP 10.1—'unless the collection is required by law'—and NPP 10.2—'where the information is collected as required or authorised by or under law'—is different. NHPP 1 of the draft *National Health Privacy Code* provides that health information may be collected without consent where the collection is 'required, authorised or permitted, whether expressly or impliedly, by or under law'.

57.107 The OPC did not support the approach in NHPP 1 on the basis that the formulation was too wide. The legal authority to collect health information without an individual's consent should be 'relatively narrow, transparent and subject to a clear statement from a Parliament'.[107]

57.108 The OPC expressed the view that the existing provisions in NPP 10.2—that allow health information to be collected without consent where necessary to provide a health service to the individual 'as required or authorised by or under law'—were appropriate. The OPC noted that the Prescription Shopping Information Service (PSIS)—established by Medicare Australia to allow registered medical practitioners to ring and find out if health consumers are 'prescription shopping' or acquiring medicines in excess of medical needs—is an example of collection that is authorised, rather than required, by or under law.[108]

57.109 DOHA expressed the view that

> as a matter of general principle it should not be considered an interference with privacy for an agency or organisation to collect health information where 'the collection is required or authorised by law'.

---

105 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 3. See also Ch 13.

106 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

107 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

108 *National Health Act 1953* (Cth) s 135AC.

ALRC's view

57.110 The proposed 'Collection' principle, discussed in detail in Chapter 18, provides that sensitive information, including health information, must not be collected without consent except where 'the collection is required or specifically authorised by or under law'. The ALRC's view is that the *Privacy Act* should not fetter a government's discretion to require or authorise that personal information, including health information, be handled in a particular way;[109] however, in relation to sensitive information, the authority to collect such information without consent should be express, rather than implied. This proposed exception should replace the exceptions currently set out in NPP 10.1(b) and NPP 10.2. This will eliminate the problem of inconsistency between these two existing provisions.

Binding rules established by health or medical bodies

57.111 NPP 10.2 also provides that health information may be collected without consent if the information is collected in order to provide a health service to the individual and in accordance with binding rules established by 'competent health or medical bodies that deal with obligations of professional confidentiality'. The draft *National Health Privacy Code* does not include this exception.

57.112 The OPC Review recommended that:

> The Australian Government should consider amending NPP 10.2(b)(ii) to clarify the nature of the binding rules intended to be covered by this provision, particularly with regard to the substantive content of such rules.[110]

57.113 In its submission, the OPC considered the exception provided by NPP 10.2(b)(ii). The OPC expressed the view that such rules would need to:

- be formally adopted by a state/territory medical board as a statement of appropriate professional practice;
- prescribe the circumstances in which the collection can or cannot occur without the patient's consent;
- define or regulate obligations of professional confidentiality in relation to the information collected; and
- provide a mechanism for sanctions for breach.

---

109 See Ch 13 for a detailed discussion of this issue.

110 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 84.

57.114 The OPC stated that:

> NPP 10.2(b)(ii) is intended to provide a mechanism to allow collection by health service providers where necessary to provide a health service, and in accordance with binding rules of professional confidentiality. However, it is the Office's view that no current rules fit the terms of 10.2(b)(ii) in such a way that it could be confidently relied upon.[111]

57.115 The NHMRC also were of the view that no such rules existed and that the provision should be deleted.[112]

ALRC's view

57.116 The ALRC notes that neither the OPC nor the NHMRC are aware of any existing 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality' that would fulfil the requirements of NPP 10.2(b)(ii). The ALRC proposes to drop the reference to this mechanism from the proposed 'Collection' principle.

Inconsistency between the collection, use and disclosure principles

57.117 Another issue raised in IP 31 was the lack of consistency between NPP 2 on use and disclosure of health information and NPP 10 on collection of health information.[113] In many communications of health information, there is both a disclosure and a collection. For example, a general practitioner collects health information for the primary purpose of providing a health service to a health consumer. The general practitioner may disclose that information to a number of other health service providers involved in treating the consumer, for example, a pathologist and a specialist.

57.118 Such disclosures are consistent with NPP 2 if they are directly related to the primary purpose of collection and within the reasonable expectations of the individual health consumer. NPP 10 requires that health information be collected with consent, although that consent may be express or implied. The issue is whether the pathologist and the specialist in the above example can rely on the implied consent of the health consumer to collect the consumer's health information.

57.119 In relation to the inconsistency between use and disclosure of health information under NPP 2 and collection of health information under NPP 10, the OPC suggested that NPP 10 should be amended to allow the collection of health information where necessary for providing a health service and where the collection was within the expectations of a reasonable person:

---

111 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
112 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
113 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [8.160].

> In the Office's view, option 3 would appear to offer an appropriate and transparent mechanism for reforming NPP 10.2(b)(ii), and would cause the least interference with current good practice in the health sector. This option would provide greater alignment between the disclosure and collection provisions of the NPPs, and resolves the possible uncertainty surrounding collection by members of a treating team and other similar scenarios.[114]

57.120 A number of other stakeholders also suggested that this matter should be clarified.[115]

ALRC's view

57.121 The ALRC notes that health information must generally be collected with consent and that consent, to be valid, must be voluntary and informed.[116] If health information is used or disclosed for the primary purpose of collection or for a directly related secondary purpose and the individual would reasonably expect the health service provider to use or disclose the information in that way, the ALRC's view is that the resulting collection by another member of the treating team, for example, a pathologist or specialist, is likely to be consistent with the express or implied consent provided at the point of original collection. Good communication between health service providers and consumers at the point of original collection would put this beyond doubt.

57.122 The ALRC recognises, however, that it is important to facilitate information flow in the health services context among members of treatment teams. The ALRC is interested in receiving further submissions on whether the proposed *Privacy (Health Information) Regulations* should provide that health information may be collected without consent where it is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information. A regulation of this nature would bring the proposed 'Collection' principle, as it applies to health information, more into line with the proposed 'Use and Disclosure' principle.

Question 57–1 Should the proposed *Privacy (Health Information) Regulations* provide that health information may be collected without consent where it is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose?

---

114 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

115 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

116 See Ch 16 for a detailed discussion of consent.

Use and disclosure of health information

Background

57.123 IPPs 10 and 11 and NPP 2 regulate the use and disclosure of personal information. IPP 10 provides that information, including health information, may be used for the particular purpose it was collected or a directly related purpose. If it is to be used for any other purpose the person who wishes to use the information must have the consent of the individual concerned. IPP 11 provides that information may not be disclosed to a person, body or agency unless the individual concerned is reasonably likely to have been aware that information of that kind is usually passed to that person, body or agency. If it is to be disclosed in other circumstances, the person who wishes to disclose the information must have the consent of the individual concerned. There are a number of exceptions to these rules, including where use or disclosure of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

57.124 NPP 2 provides that sensitive information, including health information, may not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the 'primary purpose of collection' and the individual concerned would reasonably expect the organisation to use or disclose the information for that secondary purpose. If it is to be used for any other purpose the person who wishes to use the information must have the consent of the individual concerned. There are a number of exceptions to this rule, including where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety.

57.125 NPP 2.4 makes special provision for the disclosure of health information to a person who is 'responsible' for the individual where the individual is physically or legally incapable of giving consent to the disclosure or physically cannot communicate consent to the disclosure. Such disclosures only may be made by health service providers in the health services context. The health service provider must be satisfied that the disclosure is necessary to provide appropriate care or treatment to the individual or the disclosure must be made for compassionate reasons. The disclosure must not be contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the health service provider is aware or could reasonably be expected to be aware. The disclosure must be limited to that information that it is reasonable to disclose in the circumstances.

57.126 A person is defined as 'responsible' for an individual if the person is:

- a parent of the individual;
- a child or sibling of the individual and at least 18 years old;
- a spouse or de facto spouse of the individual;

- a relative of the individual, at least 18 years old and a member of the individual's household;
- a guardian of the individual;
- exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;
- a person who has an intimate personal relationship with the individual; or
- a person nominated by the individual to be contacted in case of emergency.[117]

57.127 The *Privacy Legislation Amendment Act 2006* (Cth), passed in September 2006, amended NPP 2.1 to allow the use or disclosure of genetic information about an individual to a genetic relative in circumstances where the genetic information may reveal a serious threat to the genetic relative's life, health or safety. Any such use or disclosure will have to be done in accordance with guidelines relating to the use and disclosure of genetic information, currently under development. Section 95AA of the *Privacy Act* provides that these guidelines are to be issued by the NHMRC and approved by the Privacy Commissioner.[118]

57.128 Concern was expressed in the course of the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry)[119] and the OPC Review[120] that the concept of 'primary purpose of collection' in NPP 2 may be interpreted in a narrow way that might impede the provision of holistic health care and the appropriate management of an individual's health.

57.129 In its submission to the OPC Review, the Australian Medical Association (AMA) expressed the view that the primary purpose of collection should generally be 'to provide for the person's health care and general well being … unless another meaning is specifically agreed to between the doctor and the patient'. The AMA also noted that the primary purpose should not be limited to a particular episode of care:

> The care of a patient's health and well being is not achieved by episodic care. The process is not static, nor can it be temporally defined. One's past health and well being impacts on one's current health and well being which in turn influences one's

---

117 The terms 'child', 'parent', 'relative' and 'sibling' are defined in NPP 2.6.

118 This amendment was intended to implement, in part, Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 21–1.

119 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.63].

120 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 264–265.

> future health and well being. Health care is an on-going process that spans from conception through to death.[121]

57.130 The OPC Review stated that:

> There is an intentionally close relationship between the primary purpose and the directly related purpose provisions at NPP 2.1(a), which in this context means that with open communication between a health service provider and an individual (something to be expected in the delivery of quality health care), a holistic approach to care can be agreed either explicitly or implicitly. In other words, where the individual expects their health information to be used in the delivery of health care to them in a holistic manner, it is permissible under NPP 2.[122]

57.131 The OPC Review stated that the OPC would work with the health sector to develop further guidance about the operation of NPP 2 as it specifically relates to the issue of primary and secondary purpose in the health services context.[123]

57.132 The regime established for using and disclosing health information in NHPP 2 of the draft *National Health Privacy Code* is similar to NPP 2 in that it allows the use and disclosure of health information for the primary purpose of collection and directly related secondary purposes within the reasonable expectations of the health consumer. However, NHPP 2 also allows the use of health information without consent where all of the following apply:

> (i) the organisation is a health service provider providing a health service to the individual; and
>
> (ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and
>
> (iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and
>
> (iv) the information is used in accordance with guidelines, if any, issued for the purposes of this paragraph.

Submissions and consultations

57.133 In IP 31, the ALRC asked whether guidance by the OPC was an appropriate and effective response to concerns about the provisions of NPP 2 and the use and disclosure of health information.[124]

57.134 In its submission, the NHMRC described a number of situations in which health service providers might be unclear about their obligations under the *Privacy Act*.

---

121 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

122 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 263.

123 Ibid, recs 77–78.

124 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–17.

> For example, a patient is admitted to a hospital for acute care, and the hospital contacts the patient's general practitioner and asks him or her to disclose health information about the patient for the purpose of ongoing clinical care. There is not a serious and imminent threat to the patient's life, health or safety. The general practitioner does not have direct access to the patient to obtain consent to the disclosure of their health information. Nevertheless, good clinical practice requires its timely disclosure.[125]

57.135 The NHMRC stated that, while use or disclosure in these circumstances might well be a directly related secondary purpose, it will not always be clear to general practitioners whether individuals would reasonably expect their health information to be disclosed in these circumstances. The NHMRC was therefore of the view that use and disclosure to other health care providers of health information for the purposes of the current care of an individual health consumer should be permitted explicitly without any additional requirement that the health consumer would reasonably expect the information to be used or disclosed in this way.[126]

57.136 The Australian Nursing Federation (ANF) was of the view, however, that if health information is collected with consent and appropriate information is provided to individuals, 'then there should be little impediment to the appropriate management of the individual's health'.[127]

57.137 The OPC remained of the view that NPP 2 sits comfortably with the 'relationships of trust and good communication that are the hallmark of good practice in the health sector' and that NPP 2 does not require amendment. In its submission, the OPC suggested that it is not always, or even usually, necessary for health service providers to seek the consent of an individual before using or disclosing their health information to other members of a treatment team.[128]

57.138 The OPC also stated its view that an holistic approach to the provision of health services can be accommodated by the 'directly related secondary purpose within the reasonable expectations of the individual' test in NPP 2. The OPC noted that this test is consistent with the ethical principles set out in the AMA's Code of Ethics,[129] including respect for the individual; health care as a collaboration between doctor and patient; and patient confidentiality. The OPC did not agree that the primary purpose of collection should be broadly defined as providing 'for the person's health care and general well being', as this would allow use and disclosure of health information without taking the health consumer's reasonable expectations into account or, alternatively, seeking consent.

---

125 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
126 Ibid.
127 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.
128 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
129 Australian Medical Association, *Code of Ethics* (2004).

57.139 The OPC was not of the view that NHPP 2 provided a better framework for the use and disclosure of health information. The OPC stated that NHPP 2 was unnecessarily lengthy and complex, and that the discretions conferred by the provision did not give adequate weight to individuals' wishes and expectations about the way that their health information is used and disclosed. A number of other stakeholders, however, were more supportive of NHPP 2.[130]

57.140 The OPC reiterated the recommendations from its review that further guidance on the operation of NPP 2 in the health services context would be provided:

> This may include updating information sheets, providing greater access to these and other Office resources, and publishing articles in prominent health sector publications. A clearer understanding of how these terms operate would allow health service providers to be more confident in using and disclosing patients' information for appropriate and mutually anticipated purposes, and ensure individuals receive enough information to retain control over the direction of their healthcare.[131]

57.141 A number of other stakeholders agreed that further guidance was necessary and appropriate.[132]

ALRC's view

57.142 The ALRC supports the OPC Review recommendations that further guidance be developed for health care providers on the use and disclosure of health information in the provision of health services. There does appear to be a lack of clarity on the meaning of the principles among health service providers. This is undesirable, particularly if it is preventing the flow of health information from one health service provider to another in appropriate circumstances.

57.143 The ALRC notes the NHMRC's concern that it is unclear whether the use of an individual's health information for ongoing care would fall within the reasonable expectations of the individual. The ALRC's view is that a reasonable individual would expect their general practitioner to disclose their health information to a hospital that was providing health services to the individual in an acute care situation if the individual was not capable of giving consent. If the individual was capable of giving consent, the situation could be clearly resolved by asking the individual.

57.144 The ALRC agrees with the OPC that the situation also could be clarified with health consumers at the time that health information is originally collected, if general practitioners had concerns in this regard. The test set out in NPP 2 and incorporated in

---

130 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

131 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

132 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; A Smith, *Submission PR 79,* 2 January 2007.

the proposed 'Use and Disclosure' principle—that any secondary purpose must be directly related to the primary purpose of collection and within the reasonable expectations of the individual—is considered appropriate and workable in this context. An individual's health information should not be used without consent and outside the reasonable expectations of the individual.

Disclosure of health information to a person 'responsible'

57.145 NPPs 2.4, 2.5 and 2.6—which allow disclosure in the health services context to a person 'responsible' for an individual in certain circumstances—did not attract comment in submissions and consultations. The ALRC proposes a number of changes to the provisions, however, including as a consequence of the proposals put forward in Chapter 61 in relation to adults with a decision-making disability. The first change is that these provisions should be moved to the *Privacy (Health Information) Regulations*. The provisions deal only with health information in the health services context and, as discussed in Chapter 56, the ALRC's view is that such provisions should not be included in the text of the proposed UPPs.

57.146 The second change concerns the term 'physically or legally incapable of giving consent to the disclosure or physically cannot communicate consent to the disclosure'. In Chapter 61, the ALRC proposes that the *Privacy Act* define what it means to be incapable of giving consent, making a request or exercising a right under the Act. The proposed *Privacy (Health Information) Regulation* should simply state that an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if the individual is 'incapable of giving consent'.

57.147 The remaining proposals relate to the definition of a 'responsible' person. In Chapter 61, the ALRC proposes that the *Privacy Act* be amended to include an 'authorised representative' mechanism. Where an individual is incapable of giving consent, making a request or exercising a right under the Act, then an authorised representative of that individual may do this on behalf of the individual.[133]

57.148 The definition of 'responsible person' should be amended to include a reference to 'authorised representative'. To avoid duplication, those elements that fall within the proposed definition of 'authorised representative'—such as a guardian appointed under law or an attorney appointed under an enduring power of attorney—should be omitted from the definition of 'responsible person'. As the proposed definition of 'authorised representative' only includes a person with parental responsibility for the individual if the individual is under 18, the definition of a person 'responsible' should continue to include a reference to a parent of the individual to ensure that parents of individuals over 18 are not excluded.

---

133 Proposal 61–1.

57.149 The remaining elements of the definition of 'responsible person' should be set out expressly. In order to provide consistency across federal legislation, the reference to 'de facto spouse' should be changed to 'de facto partner', in line with recommendations made in the report, *Uniform Evidence Law* (ALRC 102).[134]

Use and disclosure of genetic information

57.150 In relation to NPP 2.1(ea)—which allows the use or disclosure of genetic information where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative—the ALRC's view is that the provision should be moved to the proposed *Privacy (Health Information) Regulations*. The proposed regulation should be expressed to apply to both agencies and organisations.

57.151 NPP 2.1(ea) provides that any use or disclosure must be in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner. Consistent with proposals in Chapter 44, the ALRC suggests that this provision be amended to provide that any use or disclosure is in accordance with binding rules issued by the Privacy Commissioner.[135] The Privacy Commissioner would be free to develop the rules in consultation with the NHMRC and other relevant stakeholders.

Proposal 57–4 The provisions of National Privacy Principle 2 dealing with the disclosure of health information in the health services context to a person responsible for an individual should be moved to the *Privacy (Health Information) Regulations*. The proposed regulation should:

(a) be expressed to apply to both agencies and organisations;

(b) provide that an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if the individual is 'incapable of giving consent' to the disclosure and all the other circumstances currently set out in NPP 2.4 are met;

(c) include a definition of a person 'responsible' for an individual amended to incorporate the term 'authorised representative'; and

(d) refer to 'de facto partner' rather than 'de facto spouse'.

134 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Rec 4–4.

135 Proposal 44–2.

Proposal 57–5 National Privacy Principle 2.1(ea) on the use and disclosure of genetic information should be moved to the *Privacy (Health Information) Regulations* and amended to apply to both agencies and organisations. Any use or disclosure under the proposed regulation should be in accordance with binding rules issued by the Privacy Commissioner.

Access to health information

Background

57.152 In *Breen v Williams*,[136] the High Court of Australia unanimously held that health consumers do not have a right of access to their medical records at common law. Consequently, health consumers must rely on legislation, including the *Privacy Act*, to provide them a right of access to the health information held in medical records.

57.153 IPP 6 provides in relation to agencies that:

> Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

57.154 The extent of the exceptions to IPP 6 are somewhat unclear but include, for example, those situations in which a record-keeper is required or authorised to refuse access under the FOI Act and the *Archives Act 1983* (Cth). Chapter 12 considers how this legislation, including the exemptions set out in the legislation, interacts with the *Privacy Act*.

57.155 NPP 6 provides that organisations must provide individuals with access to their personal information on request, subject to a number of exceptions. In the case of health information, organisations are not required to provide access if doing so would pose a serious threat to the life or health of any individual.[137] The list of exceptions also includes situations in which: providing access would have an unreasonable impact on the privacy of other individuals;[138] the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery;[139] and denying access is required or authorised by or under law.[140]

---

136 *Breen v Williams* (1996) 186 CLR 71.
137 *Privacy Act 1988* (Cth) sch 3, NPP 6.1(b).
138 Ibid sch 3, NPP 6.1(c).
139 Ibid sch 3, NPP 6.1(e).
140 Ibid sch 3, NPP 6.1(h).

57.156 Both health consumers and health service providers appear to have concerns relating to access to health information. Of the 330 complaints under the NPPs against health care providers received by the OPC between 21 December 2001 and 31 January 2005, roughly half (163) concerned a refusal of access to health records.[141]

Breakdown in therapeutic relationship

57.157 In the course of the OPC Review, the AMA and the Mental Health Privacy Coalition expressed concern that, in the health care context, there are occasions when providing access to medical records could cause harm to the health consumer or interfere with the therapeutic relationship between a health consumer and a health service provider.[142] The OPC Review stated that:

> There is no doubt that there are circumstances when access to records may cause a breakdown in a therapeutic relationship and that the breakdown in the therapeutic relationship may constitute a serious risk to the patient's health.[143]

57.158 In addition, the OPC expressed the view that NPP 6.1(c)—which allows an organisation to deny access where it would have an unreasonable impact on the privacy of someone else—might be relied upon to protect health service providers' views in some circumstances. The OPC did not address expressly the situation in which access would cause a breakdown in the therapeutic relationship that did not pose a serious threat to the life or health of an individual. The OPC did not recommend an amendment to NPP 6 but expressed the view that more guidance was necessary.[144]

57.159 The draft *National Health Privacy Code* provides very detailed provisions on the process for providing access to health information and for dealing with situations in which access is refused. As discussed in Chapter 56, the ALRC's view is that this level of detail should not be included in a principles-based regime. The grounds provided in NHPP 6 for refusing access are essentially the same as those provided in NPP 6. NHPP 6 also provides, however, that where access is denied on the basis that it would pose a serious threat to the life or health of any person or would have an unreasonable impact on the privacy of other individuals, the refusal must be in accordance with guidelines, if any, issued for the purposes of the specific provisions.[145]

57.160 In IP 31, the ALRC asked whether the exception in NPP 6.1(b)—that allows access to be denied if it would pose a serious threat to the life or health of any person—was appropriate. The ALRC asked whether the exception should be extended to allow a health service provider to deny access to health information if providing access

---

141 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 112.

142 Ibid, 115.

143 Ibid, 117.

144 Ibid, rec 30.

145 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 6.1.

would pose a threat to the therapeutic relationship between the health service provider and the health consumer.[146]

Submissions and consultations

57.161 There was strong support among stakeholders for the existing exception in NPP 6.1(b) and little support for extending the exception to include threats to the therapeutic relationship alone.[147] A number of submissions noted that denying access to health information also can damage therapeutic relationships and that health consumers are always at liberty to change health service providers if the relationship does break down. The ANF was strongly of the view that:

> This exception should **NOT** be extended to allow a health service provider to deny access to health information if providing access to the information would pose a threat to the therapeutic relationship between the health service provider and the health consumer. If the therapeutic relationship is so fragile then it is not going to be improved if the health service provider refuses to provide access. There is also the potential for a person to deny access for an improper purpose eg the information reveals an adverse event, inappropriate care or treatment or other information that a person may be entitled to have.[148]

57.162 The OPC stated that NPP 6.1(b) is an appropriate and effective exception, and should not be extended to include threats to the therapeutic relationship alone.

> The fact that the threat must be 'serious' reflects the principle that access to one's own personal information should be the rule, rather than the exception. At the same time the exception is broad enough to encompass serious threats to any relevant person (including threats to mental health), such as the individual themselves, other patients, practitioners and staff, and the individual's family. Similar language is used in the equivalent exceptions under NSW and Victorian health records legislation.[149]

57.163 The OPC suggested, however, that the phrase 'would pose a serious threat' requires a degree of certainty that may not always be achievable in clinical environments. It is not always possible to predict how a health consumer will react to being granted access to their health information. On this basis, the OPC suggested an alternative test of 'reasonably likely to pose a serious threat'.

---

146 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 8–20.

147 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Office of the Information Commissioner (Northern Territory), *Submission PR 103,* 15 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

148 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.

149 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

ALRC's view

57.164 There was very little support for extending the exception in NPP 6.1(b) to include a threat to the therapeutic relationship. The ALRC is not, therefore, proposing this change.

57.165 The ALRC agrees with the OPC that the current test—'providing access would pose a serious threat to the life or health of any individual'—requires a level of certainty that may be very difficult to establish. The proposed 'Access and Correction' principle, discussed in detail in Chapter 26, has adopted the approach suggested by the OPC. The proposed principle provides in part that, if an individual requests access to personal information held by an organisation, the organisation must respond within a reasonable time and provide the individual with access to the information—except to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.[150]

57.166 It is also important to note that the proposed 'Access and Correction' principle is limited to personal information held by organisations. The ALRC has formed the view that the rules relating to access and correction in respect of personal information held by agencies should be set out in a separate Part of the *Privacy Act*. These proposed provisions are discussed in detail in Chapter 12.

Use of intermediaries

57.167 The IPPs do not provide a mechanism for dealing with the situation in which access to information is denied. A consumer denied access to health information by an agency could, however, lodge a complaint with the Privacy Commissioner under s 36 of the *Privacy Act*.

57.168 By contrast, NPP 6.3 sets out a process involving the use of intermediaries to assist in situations in which access is denied.

> If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

57.169 The OPC Review noted that this right is very limited.[151] Organisations are only required to consider whether the use of an intermediary would meet the needs of the parties but are not required to take any action. There is a stronger right to the use of an intermediary in the draft *National Health Privacy Code* where access is refused on the ground that providing access would pose a serious threat to the life or health of the individual. A health service provider may offer to discuss information with the consumer or nominate a suitably qualified health service provider to discuss the

---

150 Proposal 26–6.

151 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 117.

information with the individual. If this does not occur, or the health consumer is not satisfied with the process, the health consumer may nominate a health service provider to act as intermediary.

57.170 Once an intermediary has been appointed, the health service provider must provide the intermediary with the individual's health information. The intermediary may then, among other things, consider the validity of the refusal to grant access and, if he or she thinks it appropriate to do so, discuss the content of the health information with the individual.[152]

Submissions and consultations

57.171 The ANF expressed the view that:

> There remains significant resistance across the health system in granting access to health consumers to their personal health information that will require major culture change. Whether it is in relation to fear of revealing litigable conduct or health professional censure; or is part of the characteristic paternalism that is linked to benevolence that has been a feature of the provision of health services over many years, is neither here nor there. It does, however indicate that there needs to be significant efforts made to inform and actively assist that culture to change.[153]

57.172 Although the OPC was generally of the view that the provisions in the draft *National Health Privacy Code* dealing with access to health information were overly complex and prescriptive, the OPC did express support for stronger provisions around the use of intermediaries to assist with access to health information.[154]

57.173 The NHMRC also expressed support for amending the *Privacy Act* to provide a more explicit right to the use of an intermediary.[155]

ALRC's view

57.174 The proposed 'Access and Correction' principle, discussed in Chapter 26, provides that where an organisation denies an individual access to personal information because of one or more of the exceptions set out in the proposed principle, 'the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties'. This formulation is stronger than the existing provisions in NPP 6.3 as it requires organisations to take reasonable steps to reach a compromise involving the use of a mutually agreed intermediary,

---

152 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5 div 3.

153 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.

154 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

155 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

rather than simply requiring the organisation to consider the use of a mutually agreed intermediary.

57.175 In the health services context, the ALRC's view is that a more detailed and stringent procedure in relation to the use of intermediaries should be provided. The ALRC notes that almost half of the complaints lodged with the OPC against health service providers were in relation to access to health information and that there appears to be some resistance among health service providers to allowing health consumers access to their health information. This situation could be improved substantially if health service providers were required to refer the requested health information to a registered medical practitioner for a second opinion in relation to the question of access.

57.176 The proposed regulation, set out below, provides that where an organisation denies an individual access to his or her own health information on the ground that providing access would be reasonably likely to pose a serious threat to the life or health of any individual, the organisation must advise the individual that he or she may nominate a registered medical practitioner to be given access to the health information. Once the individual has nominated a registered medical practitioner, the organisation must provide the medical practitioner with access to the individual's health information. The medical practitioner may then assess the grounds for denying access to the health information and may provide the individual with access to the information if he or she is satisfied that to do so would not be likely to pose a serious threat to the life or health of any individual.

57.177 The proposed regulation does not currently require that the nominated medical practitioner be mutually agreed upon. The ALRC would be interested in receiving feedback on whether an organisation should have the opportunity to object to the individual's choice of nominated medical practitioner before providing access to the individual's health information.

Proposal 57–6 The *Privacy (Health Information) Regulations* should provide that, if an organisation denies an individual access to his or her own health information on the ground that providing access would be reasonably likely to pose a serious threat to the life or health of any individual, the:

(a) organisation must advise the individual that he or she may nominate a registered medical practitioner to be given access to the health information;

(b) individual may nominate a registered medical practitioner and request that the organisation provide access to the information to the nominated medical practitioner;

(c) organisation must provide access to the health information to the nominated medical practitioner; and

(d) nominated medical practitioner may assess the grounds for denying access to the health information and may provide the individual with sufficient access to the information to meet the individual's needs if he or she is satisfied that to do so would not be likely to pose a serious threat to the life or health of any individual.

Health service is sold, transferred or closed

57.178 The OPC Review also considered the issue of access to personal health information where an organisation providing health services is sold or ceases to operate, for example, where a medical practitioner retires or a practice closes.[156] In some jurisdictions, specific provision is made for the retention of medical records in these circumstances. In New South Wales, for example, outgoing medical practitioners must make reasonable efforts to ensure that medical records are kept by the medical practitioner taking over the practice or that they are provided to the patient to whom they relate.[157]

57.179 In Victoria, HPP 10 imposes express obligations on health service providers when the organisation providing the health service is to be sold, transferred or closed. These obligations include advertising in local newspapers indicating that the organisation is to be sold, transferred or closed and what the organisation proposes to do with the health information it holds.[158]

57.180 The draft *National Health Privacy Code* includes detailed provisions for dealing with health information on the transfer or closure of the practice of a health service provider. NHPP 10 requires health service providers to take reasonable steps to let health consumers know about the transfer or closure and to inform consumers about the proposed arrangements for the transfer or storage of consumers' health information.

57.181 The OPC Review noted that where a health service ceases to operate, this may also raise issues relating to data security under NPP 4. There is a risk that 'abandoned' records may not be afforded adequate levels of storage and security.[159] It is also

156 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 123.
157 *Medical Practice Regulation 2003* (NSW) reg 8.
158 *Health Records Act 2001* (Vic) s 19, HPP 10.
159 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 123.

important to ensure that health information is available to health consumers seeking health services in the future.

57.182 The OPC considered that this was an important issue that should be addressed and made the following recommendations:

> The Australian Government should consider adopting the AHMAC code as a schedule to the Privacy Act. This will address the issue of access to health records when a health service ceases to operate. (See also recommendations 13, 29 and 33.)[160]
>
> The Australian Government should consider, if the AHMAC Code is not adopted into the Privacy Act, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 10 in the AHMAC Code.[161]

Submissions and consultations

57.183 The Victorian Office of the Health Services Commissioner expressed support for a provision dealing expressly with the transfer or closure of health service practices and noted that:

> Distressed consumers have contacted HSC advising they rang their doctor to find they had closed their practice and left no forwarding contact number. Some consumers have advised HSC they last saw their doctor two or three weeks earlier, and had no notice of the closure.[162]

57.184 The OPC reiterated its view that:

> Amendment to the Privacy Act to introduce a privacy principle with a similar purpose as NHPP 10, would usefully clarify the obligations of health service providers and establish reasonable expectations for individuals on the handling of their health information in these circumstances.[163]

57.185 The NHMRC stated that:

> We strongly endorse the provisions in the draft *National Health Privacy Code* which address the management of health information on the transfer or closure of the practice of a health service provider. We understand that consumers are particularly concerned about the privacy of their health information when health care practices are acquired by larger corporate providers.
>
> We consider that maintenance of health care records is vital for the future quality health care of individuals and we also are cognisant of the risk to security of records if they are 'abandoned'.[164]

---

160 Ibid, rec 35.
161 Ibid, rec 36.
162 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.
163 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
164 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

57.186 Other stakeholders agreed that the provisions of NHPP 10 dealing with the transfer or closure of a health service practice would be a useful addition to the *Privacy Act.*[165]

ALRC's view

57.187 The ALRC recognises that it is important to ensure that health information is handled appropriately when a health service is sold, amalgamated or closed or a health service provider dies. Health consumers should be notified when an event of this nature occurs to ensure that they continue to have access to the information and that the information is not lost or left without appropriate protection.

57.188 The regulation proposed below is based on NHPP 10 and requires health service providers, or their legal representatives, to ensure that individuals are aware of the sale, amalgamation or closure of the health service, or the death of the health service provider. Individuals must be informed about the proposed arrangements for the transfer or storage of their health information.

Proposal 57–7 The *Privacy (Health Information) Regulations* should provide that where a health service practice or business is sold, amalgamated or closed down and a health service provider will not be providing health services in the new practice or business, or the provider dies, the provider, or the legal representative of the provider, must take all reasonable and appropriate steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service or the death of the health service provider; and

(b) inform them about proposed arrangements for the transfer or storage of individuals' health information.

Transfer of health information

57.189 The *Privacy Act* does not deal specifically with the transfer of health information from one health service provider to another when a health consumer changes provider. In Victoria, HPP 11 in the *Health Records Act* imposes an obligation on health service providers to provide 'a copy or written summary of the individual's health information' to another provider if requested to do so by the individual or by the new provider on behalf of the individual. NHPP 11 of the draft *National Health*

165 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

Privacy Code is in similar terms. Providing a mechanism of this sort ensures that the new health service provider has access to the health consumer's health information history and means that the health consumer does not have to rely on right of access provisions.

57.190 The OPC Review recommended that the NPPs be amended to include a new principle along the lines of NHPP 11.[166]

Submissions and consultations

57.191 The Victorian Office of the Health Services Commissioner noted that:

> Situations often occur where a medical practitioner or other health provider leaves a practice and their patients or clients follow them to their new practice. This can sometimes result in hundreds of requests for transfer of records made to the provider's old practice, and hostility between the two practices can emerge. HSC attempts to assist providers to deal with these situations, and sometimes negotiates between two practices to resolve difficulties that arise. Therefore specific provisions in relation to the transfer of health information are very important and assist in the continuity of care of the health consumer.[167]

57.192 The OPC expressed the view that introducing a provision into the *Privacy Act* along the lines of NHPP 11 would be appropriate as it would meet community expectations and would be consistent with good clinical care and continuity of treatment.[168] Other stakeholders also expressed support for including a provision in the *Privacy Act* dealing with the transfer of health information from one health service provider to another.[169]

57.193 DOHA agreed, noting that:

> The transfer of information from one health service provider to another, where an individual changes provider, is an important issue in the healthcare sector. It is consistent with good professional practice for a health service provider to respond positively to an individual's request to supply the individual's new provider with their original records (or a copy) or with a summary of the information in their records. This practice facilitates the continued availability of important health information when an individual changes health service provider, subject to the choices the individual exercises, thereby helping to ensure safe and effective healthcare for the individual.[170]

---

166 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 34.

167 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

168 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

169 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

170 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

ALRC's view

57.194 The ALRC notes the difficulties that can arise in relation to the transfer of health information from one health service provider to another when a health consumer changes provider. Health consumers should have a right to have their health information transferred in these circumstances to ensure continuity of care. The ALRC proposes, therefore, the inclusion in the *Privacy (Health Information) Regulations* of a provision along the lines of NHPP 11. The proposed regulation should provide that where an individual requests that his or her health information be transferred from one health service provider to another, the information must be transferred in full or summary form. The individual also may ask a health service provider to make the request on his or her behalf.

Proposal 57–8 The *Privacy (Health Information) Regulations* should provide that if an individual:

(a) requests that a health service provider, or the health service provider's legal representative, make the individual's health information available to another health service provider; or

(b) authorises a health service provider to request that another health service provider transfers the individual's health information to the requesting health service provider,

the health service provider must transfer the individual's health information as requested. The health information may be provided in summary form.

Management, funding and monitoring

57.195 In its submission to the OPC Review, the NHMRC stated that health information was important in three areas: the provision of health services; management activities related to the provision of health services; and the conduct of research. The NHMRC noted that management activities include, for example: quality assurance; quality improvement; policy development; planning; evaluation; and cost benefit analysis and added that:

> The availability of health information without consent for quality assurance, research, and related activities is crucial to the safety and quality of clinical care, now and in the future. These activities, while similar in nature and intent, are currently subject to complex and different requirements under the *Privacy Act*, depending on the setting in

which they are conducted and whether they are characterised as quality assurance or research.[171]

Management, funding or monitoring of a health service under the NPPs

57.196 The NPPs go some way towards acknowledging the public interest in allowing the use of health information in the management activities of health service providers and by researchers. NPP 10.3 allows the collection of health information without consent in limited circumstances for:

- research relevant to public health or public safety;
- the compilation or analysis of statistics relevant to public health or public safety; or
- the management, funding or monitoring of a health service.

57.197 Although there is some overlap between these three areas, this chapter will focus on the third—that is, the management, funding and monitoring of health services. Research is discussed in the next chapter. The compilation and analysis of statistics relevant to public health or public safety can be conducted for research purposes or for management, funding or monitoring purposes. The ALRC does not propose to deal with this issue separately in this chapter on the basis that, where the compilation or analysis of statistics is done for the purposes of the management, funding or monitoring of a health service, the activity can be subsumed in the provisions dealing with management, funding and monitoring activity.

57.198 Health information only may be collected without consent for management, funding and monitoring activities in the following circumstances. An organisation must consider whether it could use de-identified information to achieve its purpose. If this is not possible, it must be impracticable for the organisation to seek the consent of all the individuals involved. Finally, the information must be collected:

- as required by law;
- in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
- in accordance with guidelines approved by the Privacy Commissioner under s 95A of the *Privacy Act*.[172]

---

171 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

172 *Privacy Act 1988* (Cth) sch 3, NPP 10.3.

As required by law

57.199 NPP 10.3(d)(i) allows for collection of health information without consent where the collection is required by law, for example, under public health notifiable diseases legislation. The proposed 'Collection' principle allows the collection of sensitive information, including health information, without consent where the collection is required or specifically authorised by or under law.[173] The proposed 'Use and Disclosure' principle allows the use and disclosure of health information without consent where the use or disclosure is required or authorised by or under law.[174] It is not necessary, therefore, to include these elements specifically in the provision dealing with collection, use and disclosure of health information without consent for the funding, management, planning, monitoring, improvement or evaluation of a health service.

In accordance with rules on professional confidentiality

57.200 NPP 10.2 also makes reference to the requirement for 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation'. The OPC suggested that any such rules would need to:

- be formally adopted by a state/territory medical board as a statement of appropriate professional practice;
- prescribe the circumstances in which the collection can or cannot occur without the patient's consent;
- define or regulate obligations of professional confidentiality in relation to the information collected; and
- provide a mechanism for sanctions for breach.

57.201 The OPC stated that it was not aware of any existing binding rules in the health sector that would meet these criteria.[175]

In accordance with s 95A Guidelines

57.202 Section 95A allows the Privacy Commissioner to approve guidelines issued by the NHMRC in relation to the collection of health information under NPP 10.3(d)(iii) for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety or the management, funding or monitoring of a health service. Section 95A also allows the Privacy Commissioner to approve guidelines on

---

173 See Ch 18.
174 See Ch 22.
175 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

the use and disclosure of health information under NPP 2.1(d)(ii) for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety. Before approving any such guidelines, the Privacy Commissioner must be satisfied that the public interest in the collection, use or disclosure of health information without consent for these purposes substantially outweighs the public interest in maintaining the level of privacy protection afforded by the NPPs.

57.203 Currently, the guidelines issued under s 95A require HREC approval for management, funding or monitoring activities conducted relying on NPP 10.3(d)(iii). The NHMRC has noted that it is often difficult to distinguish management activities such as quality assurance in the health care context from research[176] and is of the view that, where such activities amount to research, they should always be conducted in accordance with the Section 95A Guidelines and be subject to review by a HREC.[177] For example, a hospital may collect information about surgical mortality rates for quality assurance purposes, but that information may also form the basis of a research project by hospital staff or others. The NHMRC has published some guidance on how to make the distinction between quality assurance activities and research but suggests that even in relation to quality assurance activities that 'could infringe ethical principles that guide human research, independent ethical scrutiny of such proposals should be sought.'[178]

57.204 While NPP 10 expressly provides for the collection of health information for management, funding or monitoring of a health service, NPP 2 does not expressly provide for the use or disclosure of health information for the same purpose. NPP 2 does, however, allow for the use and disclosure of health information without consent for a purpose directly related to the primary purpose for which the information was collected where the person would reasonably expect the organisation to use or disclose the information for that purpose. The OPC Review expressed the view that disclosure of health information for management activities would generally be within people's reasonable expectations.[179] In response to concerns that the position is not clear, however, the OPC Review recommended that the OPC issue guidance to clarify when organisations can disclose health information for the management, funding and monitoring of a health service.[180]

---

176 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

177 Ibid. National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

178 National Health and Medical Research Council, *When Does Quality Assurance in Health Care Require Independent Ethical Review?* (2003), 3. For the purposes of this Discussion Paper, it is necessary to distinguish between the need for compliance with privacy legislation and the need for ethical review. Ethical review may include an analysis of privacy and confidentiality issues but is also concerned with the welfare and other rights of participants.

179 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

180 Ibid, Rec 61.

Management, funding or monitoring of a health service under the IPPs

57.205 Management activities are undertaken in both the public and the private health sectors. The IPPs, however, do not make specific reference to management, funding and monitoring activities and so it is necessary to interpret the basic principles to decide whether it is possible to use health information in the public sector for such activities.

57.206 The use of health information for management activities may involve collection, use or disclosure of the information. IPP 1 allows collection of health information so long as it is for a lawful purpose, directly related to the activities of the agency. IPP 1 does not require consent to collect information, including health information. This would seem to allow collection of health information by public sector health service providers for management, funding and monitoring activities directly related to the agency's activities.

57.207 IPP 10 allows use of health information without consent for the primary purpose for which it was collected and any directly related secondary purpose. In *Information Sheet 9: Handling Health Information for Research and Management*, the OPC states that:

> Some management, funding and monitoring purposes are likely to be 'directly related' to the purpose of collection, where the primary purpose of collecting information was to provide particular health services to a person.[181]

57.208 IPP 11 allows disclosure of health information without consent where the individual concerned is reasonably likely to have been aware that health information was usually disclosed to the particular person, body or agency. As noted above, the OPC considers that disclosure of health information for management activities would generally be within people's reasonable expectations.

State and territory legislation

57.209 Both the New South Wales *Health Records and Information Privacy Act* and the Victorian *Health Records Act* make express provision for the use or disclosure of health information without consent in the public and private sectors for the funding, management, planning, monitoring, improvement or evaluation of health services or training provided by a health service provider to its employees or others working with the organisation.[182] Any such use or disclosure is subject to certain criteria, for example, it must be impracticable to seek individuals' consent and reasonable steps must be taken to de-identify the information. Use or disclosure of health information

---

181 Office of the Federal Privacy Commissioner, *Handling Health Information for Research and Management*, Information Sheet 9 (2001).

182 *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 10; *Health Records Act 2001* (Vic) sch 1, HPP 2.2.

for management activities under these Acts does not depend on establishing that it is a directly related secondary purpose or that it would be within the individual's reasonable expectations.

Submissions and consultations

57.210 The OPC expressed the view that the *Privacy Act* already allows for the collection, use and disclosure of health information without consent for management, monitoring and funding activities by agencies and organisations. This position is in part based on the view that such activities are directly related to the primary purpose of collection and that individuals would reasonably expect their health information to be used and disclosed in this way. As noted above, the OPC has undertaken to issue further guidance on the matter.[183]

57.211 The NHMRC submitted, however, that:

> The complexity of these provisions has not been resolved for NHMRC stakeholders by the guidance provided to date by the Office of the Privacy Commissioner, partly because of the restrictions imposed by the 'reasonable expectation' requirement on the circumstances in which health information can be used or disclosed for quality assurance and related activities, and partly because of the underlying inconsistencies in relation to disclosure on the one hand and collection on the other. Much greater clarity of the status of these important activities is required.[184]

57.212 A number of other stakeholders also expressed the view that further guidance from the OPC would not be an adequate response to the lack of clarity in this area. These stakeholders supported amending the *Privacy Act* to deal expressly with the collection, use and disclosure of health information for management activities.[185]

57.213 The NHMRC also expressed the view that:

> The use of health information by or on behalf of an agency or organisation in which it has been collected, for the purposes of quality assurance and related activities (including management, funding, monitoring, policy development, planning, evaluation and cost-benefit analysis) should be permitted explicitly by the *Privacy Act* as an activity that is in the overall public interest, even in circumstances where it is not possible to conclude that such use is within the reasonable expectation of the person to whom the information relates.

57.214 The NHMRC and the Australian Commission on Safety and Quality in Health Care (ACSQHC) suggested that collection, use and disclosure of health information without consent for management activities be allowed where it is conducted in accordance with guidelines issued by the Privacy Commissioner or, alternatively, a PID issued by the Privacy Commissioner. Both stakeholders also expressed the view

---

183 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

184 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

185 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

that some of this activity could legitimately proceed without being subject to review by an HREC.[186]

57.215 The Australian Privacy Foundation expressed concern that

> management, funding and monitoring of health services are too broad concepts for an exception to the normal requirements for consent, express legal authority etc. Almost any activity could be encapsulated by these three terms, and they effectively allow governments to use detailed health information about individuals for a wider range of secondary purposes for which de-identified information should suffice.[187]

57.216 In its submission, the ACSQHC highlighted the importance of linking existing health information data sets to enable trends and indicators of the quality and safety of health care to be calculated and monitored. The submission notes that, for most quality and safety indicators, a probabilistic matching process can be used, and individuals are not uniquely identified. For example, it is not necessary for the purposes of data analysis to be able to say, with 100 percent accuracy, that there is a definite match between hospital admission data and death registry data.[188]

57.217 A final issue that was raised by the Australian Health Insurance Association (AHIA) was the use of health information to report on the charging practices and performance of health service providers.

> At present the National Privacy Principles (NPPs) are interpreted to mean that health funds must have the consent of practitioners to disclose their billing practices or information on the number and types of procedures and other services they perform. This can be regarded as business rather than personal information and it must be questioned whether this was the intended effect of the privacy laws and NPPs.[189]

57.218 The OPC has stated that if an individual's identity can be determined from business information, then the information is personal information for the purposes of the *Privacy Act*. Where this information is sensitive information, including health information, it will generally have to be collected with consent.[190]

57.219 The AHIA noted the following recommendations of the Taskforce on Reducing the Regulatory Burden on Business:

---

186 Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

187 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

188 Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007.

189 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

190 Office of the Privacy Commissioner, *Frequently Asked Questions: When is Business Information Covered by the Privacy Act?* <www.privacy.gov.au/faqs/bf/q8.html> at 30 July 2007.

> The Australian Government should facilitate the publication of industry-wide data on the charging practices of individual medical specialists.[191]
>
> The Australian Government should amend laws to enable data on hospital treatment outcomes to be published.[192]

57.220 In August 2006, the Australian Government agreed in principle with these recommendations and undertook to improve the information available to health consumers. It made clear, however, that:

> Information about doctors' fees needs to be considered sensitively as it relates directly to the charging practices of medical specialists, and impacts directly on the interface between the medical provider and the consumer … [and] proposals to publish data on hospital treatment outcomes need to be considered sensitively as they relate to the clinical outcomes of decisions made by health care providers.[193]

57.221 Although the *Privacy Act* impacts on the publication of this kind of information, the issue is not, primarily, a privacy issue. As noted in the Australian Government response to *Rethinking Regulation*, the publication of detailed information on the charging practices and performance of health service providers is likely to have industry wide implications and any proposed reform will need to take these implications into account. A detailed consideration of these issues falls outside the terms of reference for this Inquiry. While the *Privacy Act* would not stand in the way of this kind of regulatory reform, in the absence of such reform the *Privacy Act* will apply to such information.[194]

ALRC's view

57.222 In the ALRC's view, there is a public interest in allowing the collection, use and disclosure of health information for the funding, management, planning, monitoring, improvement or evaluation of health services in defined circumstances. The ALRC agrees that, generally, these activities can and should be conducted either on the basis of consent or using health information that does not identify individuals. The proposal below makes clear that identifiable health information only may be used where the purpose cannot be achieved using information that does not identify individuals. In addition, it must be impracticable to seek the individuals' consent and any collection, use or disclosure must be conducted in accordance with binding rules issued by the Privacy Commissioner.

57.223 The ALRC is not persuaded that individuals generally would be aware that or expect their health information to be collected, used and disclosed without consent for such activities. This gives rise to uncertainty as to whether such activity is currently

---

191 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), rec 4.11.

192 Ibid, rec 4.12.

193 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 5–6.

194 This issue is also discussed in Chs 3 and 50.

allowed by the IPPs and NPPs. The issue should be clarified in the proposed UPPs, as amended by the *Privacy (Health Information) Regulations.* The ALRC has adopted the more detailed description of management, funding and monitoring activities from the draft *National Health Privacy Code*—that is, funding, management, planning, monitoring, improvement or evaluation of health services—to make clear that health information can also be used to evaluate and improve the provision of health services.[195]

57.224 The proposed rules to be issued by the Privacy Commissioner are intended to replace the provision in NPP 10.3(d)(ii) that allows collection of health information without consent for management, funding or monitoring of a health service where it is conducted 'in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality'. The ALRC notes that the OPC is not aware of the existence of any such binding rules in the health sector.

57.225 The proposed rules are intended to replace, in some circumstances, the provision in NPP 10.3(d)(iii) allowing collection of health information without consent for management, funding or monitoring of a health service where it is conducted in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner under s 95A of the *Privacy Act*. The NHMRC has noted that some management activity does not amount to research and does not require review by an HREC.[196] In the ALRC's view, in these circumstances the activity should be able to proceed simply on the basis of rules issued by the Privacy Commissioner.

57.226 The proposed rules could address issues such as: who may collect, use and disclose identified health information without consent for management activities; limits on further use and disclosure of the information; requirements to destroy information, and requirements to render health information non-identifiable before publication of any papers or reports.

57.227 The ALRC notes that some funding, management, planning, monitoring, improvement and evaluation of health service activities also may be characterised as research. Where particular activities can be characterised as both management activities and research the ALRC is of the view that the activity should be conducted in accordance with the proposed rules issued by the Privacy Commissioner and should also be subject to the provisions relating to research, discussed in the following chapter. The proposed research provisions, like the s 95 and s 95A guidelines, provide for review of research proposals by an HREC.

---

195 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) NHPP 2.2(f)(i).

196 National Health and Medical Research Council, *When Does Quality Assurance in Health Care Require Independent Ethical Review?* (2003), 5.

57.228 Finally, it is also possible that some management activity, while not amounting to research, may still require ethical review. The NHMRC has provided guidance on when this might be necessary, for example, where a proposed quality assurance activity poses risks for, or imposes burdens on, health consumers beyond those of their routine care.[197] The ALRC notes this advice, although the broader issue of ethical review of management activities is outside the Inquiry's terms of reference.

57.229 The New South Wales and Victorian health privacy legislation and the draft *National Health Privacy Code* allow the use of health information without consent for training purposes in some circumstances.[198] In the ALRC's view, the public interest balance in relation to training activities is not the same as the public interest balance in ensuring the quality and safety of healthcare. Health information used in the training context should be used in accordance with the proposed UPPs and special provision should not be made for this activity.

57.230 Finally, health consumers should be made aware, as far as possible, that their health information may be used without consent for the funding, management, planning, monitoring, improvement or evaluation of a health service.

Proposal 57–9 The *Privacy (Health Information) Regulations* should make express provision for the collection, use and disclosure of health information without consent where necessary for the funding, management, planning, monitoring, improvement or evaluation of a health service where:

(a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual;

(b) it is impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

(c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

Proposal 57–10 The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, improvement or evaluation of a health service.

197 Ibid, 6.

198 *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 10(1)(e); *Health Records Act 2001* (Vic) sch 1, HPP2.2(f)(ii); National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) NHPP 2.2(f)(ii).

58. Research

Contents

Introduction 1653
The current arrangements 1654
- Health and medical research 1654
- Consent 1657
- Information Privacy Principles 1658
- National Privacy Principles 1658
- Section 95 and 95A Guidelines 1659

Research other than health and medical research 1663
Definition of research 1667
The public interest balance 1670
Impracticable to seek consent 1676
Human Research Ethics Committees 1681
An exception to the proposed Unified Privacy Principles 1689
Identifiable personal information 1692
Databases and data linkage 1699
- Establishing databases 1699
- Using and linking information in databases 1705

Introduction

58.1 This chapter examines the special arrangements in place under the *Privacy Act 1988* (Cth) to allow for the use of personal information in health and medical research. The Act currently provides for the use of personal information, including health information, without consent, for health or medical research where the research is conducted in accordance with guidelines issued by the National Health and Medical Research Council (NHMRC) and approved by the Privacy Commissioner. These arrangements recognise that, in some circumstances, the public interest in allowing particular research projects to proceed outweighs the public interest in maintaining the level of privacy protection provided by the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs).

58.2 These arrangements are currently limited to the use of personal information for medical research under the IPPs, and the use of health information for research, or the compilation or analysis of statistics, relevant to public health or public safety under the NPPs. The chapter considers whether the arrangements should be extended to include

the use of personal information in other sorts of research in areas such as criminology and sociology.

The current arrangements

Health and medical research

58.3 The Hon Tony Abbott MP, Minister for Health and Ageing, noted in 2004 that:

> Australia is a world leader in health and medical research. On a per capita basis, our research output is twice the OECD average, even though we spend much less, per capita, than the UK or the USA.
>
> Investment in health and medical research makes good economic and health sense. It generates significant returns both in terms of health benefits—longevity and increased quality of life for Australian people generally; and economic benefits, through increased knowledge based jobs and economic activity.[1]

58.4 There is strong community support for health and medical research. 90% of voters in a survey conducted for Research Australia in 2006 thought that health and medical research would play an important role in Australia's future. Survey participants ranked health and medical research equal sixth on a list of 24 issues the Australian Government should be focusing on alongside reducing crime and improving law and order and increasing funding for preventive health care.[2]

58.5 The NHMRC plays an important role in fostering health and medical research in Australia. The NHMRC is a statutory authority, within the portfolio responsibilities of the Minister for Health and Ageing, established by the *National Health and Medical Research Council Act 1992* (Cth) (the NHMRC Act). The Act provides that the role of the NHMRC is to:

- raise the standard of individual and public health throughout Australia;
- foster the development of consistent health standards between the various states and territories;
- foster medical research and training and public health research and training throughout Australia; and
- foster consideration of ethical issues relating to health.[3]

58.6 The NHMRC is also the peak funding and advisory body for health and medical research in Australia and makes recommendations to the Minister for Health and Ageing on funding of health and medical research and training. Australian Government

---

1 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), Minister's Forward.

2 Research Australia, *Health and Medical Research Public Opinion Poll 2006* (2006).

3 *National Health and Medical Research Council Act 1992* (Cth) s 3.

funding of health and medical research is primarily provided from the Medical Research Endowment Account established under the NHMRC Act.[4] Some funding is also provided through the Australian Research Council and other schemes. The NHMRC notes that the Australian Government has more than doubled investment in health and medical research since 1999.[5] Funding in 2006–07 was $627.2 million.[6]

58.7 In a 2004 report, the Investment Review of Health and Medical Research Committee estimated that, in 2000–01, of the $1.7 billion invested in Australian health and medical research, 47% was provided by the Australian Government, 44% by the private sector and 9% by state and local government.[7]

58.8 The report noted that the bulk of Australian Government investment in this period was directed to the higher education sector, although some of this research was then performed by, or in conjunction with, other institutions. Smaller amounts were spent by the Australian Government directly through agencies such as the Department of Health and Ageing (DOHA) and the Commonwealth Scientific and Industrial Research Organization (CSIRO), or channelled to businesses or non-profit groups. State governments spent the bulk of their investment in their own institutions, including state departments of health, medical research institutes and public hospitals. The business sector largely funded its own research. The non-profit sector funded half of its research from its own fund raising, and the other half through investment from the Australian Government, state governments and business.[8]

58.9 The NHMRC noted in its submission to the Office of the Privacy Commissioner's (OPC) review of the private sector provisions of the *Privacy Act* (the OPC Review) that:

> Consistent with patterns of the provision of clinical care, the conduct of health and medical research in the Australian health care system frequently spans the public and private sectors.
>
> Much health and medical research is multi-site or multi-jurisdictional, involving participants who move between the public and private health sectors.[9]

58.10 Under the NHMRC Act, the Australian Health Ethics Committee (AHEC)—a principal committee of the NHMRC—has responsibility for developing guidelines for

---

4 Ibid pt 7.

5 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 1 August 2007.

6 National Health and Medical Research Council, *Correspondence*, 19 April 2007.

7 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), 17.

8 Ibid, 17.

9 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

the ethical conduct of medical research.[10] The primary set of guidelines for human research, developed jointly by the NHMRC, the Australian Research Council and the Australian Vice Chancellors' Committee (AVCC), is the 2007 *National Statement on Ethical Conduct in Human Research*[11] (the National Statement). This National Statement replaces the 1999 *National Statement on the Ethical Conduct in Research Involving Humans* and was developed following extensive public consultation and debate.

58.11 The National Statement sets out ethical principles relevant to research involving humans and guidance on the formation, membership and functions of Human Research Ethics Committees (HRECs). It is important to note that, while the guidelines in the National Statement that are applicable to the conduct of health and medical research involving humans are issued by the NHMRC in fulfilment of its statutory obligations, the National Statement applies to all research involving humans, not just health and medical research.

58.12 The National Statement provides that any research proposals involving more than a low level of risk to participants must be reviewed and approved by an HREC. It also sets out requirements to be followed by:

- institutions or organisations in establishing HRECs;
- researchers in submitting research proposals to HRECs; and
- HRECs in considering and reaching decisions regarding research proposals and in monitoring the conduct of approved research.

58.13 Although the National Statement is not legally binding, the Statement stipulates that it must be used to inform the design, ethical review and conduct of human research that is funded by, or takes place under the auspices of, the NHMRC, the Australian Research Council or the AVCC. Compliance with the National Statement is a condition of NHMRC grants of research funds.[12] In order for an institution to apply to be an NHMRC Administering Institution for the purposes of applying for, and subsequently administering, NHMRC research funds, all research conducted within the institution, whether funded by the NHMRC or not, must comply with the National Statement.[13]

---

10 *National Health and Medical Research Council Act 1992* (Cth) s 35(3).

11 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

12 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [14.1]–[14.8]. The power to withdraw funding is the most important and direct mechanism by which the NHMRC may induce compliance with the National Statement. As noted above, however, not all health and medical research is funded by the Australian Government on the advice of the NHMRC. The issue of enforcing compliance with the National Statement was considered in detail in ALRC 96, Ch 14.

13 National Health and Medical Research Council, *Administering Institutions Policy*, 6.

58.14 As discussed below, the *Privacy Act* regime incorporates the HREC approval process established by the National Statement to ensure that where research is conducted using personal information without consent, that research is conducted with due regard for the protection of that information.

Consent

58.15 The conduct of health and medical research frequently involves the collection and use of personal information about individuals. Generally, individuals who participate in research projects do so on the basis of consent and, in these circumstances, it is possible to handle participants' personal information in compliance with the IPPs or the NPPs. The National Statement makes clear that:

> Respect for human beings involves giving due scope to people's capacity to make their own decisions. In the research context, this normally requires that participation be the result of a choice made by participants—commonly known as 'the requirement for consent'. This requirement has the following conditions: consent should be a voluntary choice, and should be based on sufficient information and adequate understanding of both the proposed research and the implications of participation in it.[14]

58.16 The *Privacy Act*, however, like the National Statement, recognises that in some circumstances it is very difficult or impossible to conduct research that may be in the public interest—for example, epidemiological studies of the distribution and determinants of disease in large populations—in a way that complies with the IPPs and the NPPs. As CSIRO has noted:

> Informed consent and opt-in is a good model for clinical trials, for example, where the risk is normally predominantly to the participating individual. However, in the case of population health research, the findings will often be implemented for the whole population. In these cases informed consent and opt-in may not be good models because non-participation can introduce bias and therefore affect the applicability of the results.[15]

58.17 The *Privacy Act* provides a mechanism to allow such research to go forward, subject to guidelines issued by the NHMRC and approved by the Privacy Commissioner. The concept of consent under the *Privacy Act* is discussed in detail in Chapter 16.

58.18 The *Privacy Act* provides for two sets of binding guidelines in the area of health and medical research: one set of guidelines binding on public sector agencies made under s 95 of the Act, and one set of guidelines binding on private sector organisations made under s 95A. Sections 95 and 95A both require the Privacy Commissioner to be

---

14 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 19.

15 CSIRO, *Submission PR 176,* 6 February 2007.

satisfied before approving the guidelines that the public interest in the relevant research outweighs to a substantial degree the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs.

Information Privacy Principles

58.19 The IPPs themselves do not refer to the use of personal information for health and medical research. Section 95 of the *Privacy Act*, however, provides as follows:

> (1) The CEO of the National Health and Medical Research Council may, with the approval of the Commissioner, issue guidelines for the protection of privacy in the conduct of medical research.
>
> (2) The Commissioner shall not approve the issue of guidelines unless he or she is satisfied that the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence to the Information Privacy Principles.
>
> (3) Guidelines shall be issued by being published in the *Gazette*.
>
> (4) Where:
>
> (a) but for this subsection, an act done by an agency would breach an Information Privacy Principle; and
>
> (b) the act is done in the course of medical research and in accordance with guidelines under subsection (1);
>
> the act shall be regarded as not breaching that Information Privacy Principle.
>
> (5) Where the Commissioner refuses to approve the issue of guidelines under subsection (1), an application may be made to the Administrative Appeals Tribunal for review of the Commissioner's decision.

58.20 The current *Guidelines under Section 95 of the Privacy Act 1988*[16] (Section 95 Guidelines) were issued in 2000. Once these guidelines were approved by the Privacy Commissioner and published in the Australian Government *Gazette*, they gained the force of law. If an agency does an act in the course of medical research that would have breached the IPPs but is consistent with the Section 95 Guidelines, the act is regarded as not breaching the IPPs.

National Privacy Principles

58.21 The NPPs, unlike the IPPs, specifically provide for the use of health information in research. NPPs 2 and 10 provide that health information may be collected, used and disclosed where necessary for research or the compilation or analysis of statistics, relevant to public health or public safety where:

---

16 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000).

- the purpose cannot be served by the collection of information that does not identify the individual;[17]

- it is impracticable for the organisation to seek the individual's consent to the collection, use or disclosure;[18]

- the information is collected, used and disclosed in accordance with guidelines approved under s 95A;[19]

- in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;[20] and

- the organisation takes reasonable steps to permanently de-identify the information before it discloses it.[21]

58.22 Section 95A of the *Privacy Act* provides a similar mechanism to s 95. The current *Guidelines Approved under Section 95A of the Privacy Act 1988*[22] (Section 95A Guidelines) were issued in 2001.

Section 95 and 95A Guidelines

58.23 Both the Section 95 and 95A Guidelines provide a detailed framework within which HRECs must consider the privacy implications of research proposals involving the use of individuals' personal or health information. HRECs may approve research proposals seeking to use identifiable personal or health information without consent only on the basis that the public interest in the research substantially outweighs the public interest in maintaining the level of privacy protection provided by the IPPs and the NPPs.

58.24 The guidelines also address issues such as procedures to be followed in preparing a proposal for approval by an HREC and procedures to be followed in the collection, use or disclosure of personal or health information for research or the compilation or analysis of statistics.

58.25 The Section 95 and 95A Guidelines do not apply to the collection, use and disclosure of health information by agencies or organisations that are not covered by

17 *Privacy Act 1988* (Cth) sch 3, NPP 10.3(b).
18 Ibid sch 3, NPPs 2.1(d)(i), 10.3(c).
19 Ibid sch 3, NPPs 2.1(d)(ii), 10.3(d).
20 Ibid sch 3, NPP 2.1(d)(iii).
21 Ibid sch 3, NPP 10.4.
22 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

the *Privacy Act*. For example, the *Privacy Act* does not apply to state public sector entities, including public teaching hospitals and associated research bodies, where such bodies are established for a public purpose under a law of a state.[23] These organisations, however, may be covered by state legislation.[24]

58.26 Because the Section 95 and 95A Guidelines relate to the IPPs and the NPPs, respectively, and because of differences in the enabling provisions, the guidelines are not identical. The OPC Review noted stakeholder views that having two sets of guidelines gives rise to inconsistency and confusion leading to conservative and incorrect decision making.[25] The NHMRC expressed the view that this was hindering the conduct of effective health and medical research.[26]

58.27 A number of stakeholders, including the NHMRC, expressed strong support for a single set of principles and a single set of guidelines regulating health information in the conduct of health and medical research.[27] In response, the OPC Review stated that 'the *Privacy Act* is not intended to restrict important medical research'[28] and made the following recommendation:

> As part of a broader inquiry into the *Privacy Act* (see recommendation 1), the Australian Government should consider … how to achieve greater consistency in regulating research activities under the *Privacy Act*.[29]

58.28 As discussed in Chapter 56, between 2000 and 2004, the Australian Health Ministers' Advisory Council (AHMAC) National Health Privacy Working Group developed a draft *National Health Privacy Code* that includes a set of National Health Privacy Principles (NHPPs). The draft Code provides a single regime for the collection, use and disclosure of health information for 'research, or the compilation or analysis of statistics, in the public interest'. For example, NHPP 1 provides in relation to collection of health information that:

> An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies—
>
> … if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest—

---

23 *Privacy Act 1988* (Cth) s 6C.

24 See, eg, *Health Records Act 2001* (Vic) HPPs 1.1(e)(iii), 2.2(g)(iii).

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 201.

26 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

27 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006; Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Australian Academy of Science, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 18 January 2005.

28 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 199.

29 Ibid, rec 62 (in part).

> (i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
>
> (ii) it is impracticable for the organisation to seek the individual's consent to the collection; and
>
> (iii) the information is collected in accordance with guidelines issued for the purposes of this sub-paragraph.[30]

58.29 NHPP 2 provides similar criteria for the use and disclosure of health information for research with some additional safeguards around disclosure.[31] The revised draft Code also included draft mandatory guidelines for research.[32] As discussed in Chapter 56, the Code was intended to apply to all health service providers, agencies and organisations that collect, hold or use health information across the public and private sectors, and in every Australian state and territory, including in the field of health and medical research. Under this proposed regime, one set of principles and one set of guidelines would regulate health and medical research across Australia.

Submissions and consultations

58.30 Submissions and consultations made clear that having two different regimes regulating health and medical research under the IPPs and the NPPs and, in particular, two sets of guidelines, the Section 95 and 95A Guidelines, creates confusion and adds significantly to the cost and complexity of seeking approval to conduct research. There was clear support in submissions and consultations for the development of a unified regime to regulate health and medical research, including a single set of guidelines.[33]

58.31 The CSIRO stated that:

> The current policy environment regarding privacy of personal information is complex and difficult to navigate. It is quite time-consuming to ensure that a given project will be compliant with all of the relevant legislation and codes of practice. This can add significantly to the set up costs of research projects, particularly where they involve health data. In addition, and most importantly, it also means that there is a delay of up to two years in initiating research projects, and a corresponding delay in the Australian people and society's acquisition of the benefits of the research outcomes.[34]

---

30 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) sch 1, NHPP 1.1(e).

31 Ibid sch 1, NHPP 2.2(g).

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

33 Australian Commission on Safety and Quality in Health Care, *Submission PR 252,* 14 March 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

34 CSIRO, *Submission PR 176,* 6 February 2007.

58.32 In its submission DOHA stated that:

> Recent reports on the operation of the *Privacy Act* and on research have both concluded that the present fragmentation and inconsistency in privacy regulation is proving to be a major impediment to health and medical research.
>
> The Department supports the development of a single set of guidelines regulating health information in the conduct of research, to support these activities at the institutional, multi-institutional and national levels. In keeping with the objective of achieving national consistency, there should also be alignment between the privacy principles covering research and the NHMRC's *National Statement on Ethical Conduct in Human Research* (National Statement).[35]

ALRC's view

58.33 The ALRC agrees that the arrangements under the *Privacy Act* for conducting research using identifiable personal information without consent should be streamlined. The issues of complexity, fragmentation and inconsistency in the privacy regime are discussed in detail in Part C of this Discussion Paper. Chapter 4 includes a number of proposals aimed at achieving greater national consistency. Part D proposes a single set of Unified Privacy Principles (UPPs) applying to agencies and organisations. A nationally consistent privacy regime applying to both agencies and organisations and including a single set of UPPs would eliminate the need for two sets of guidelines.

58.34 In Proposals 58–8 and 58–9, below, the ALRC suggests that the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle in the UPPs should include exceptions for the conduct of research using identified or identifiable personal information without consent. These proposed exceptions provide that such research be subject to HREC review and, in addition, that such research be conducted in accordance with binding rules to be issued by the Privacy Commissioner.

58.35 In Chapter 44, the ALRC examines in detail the powers of the Privacy Commissioner to issue binding rules and non-binding guidelines and expresses the view that the *Privacy Act* should clearly distinguish between those that are advisory only and those that operate as mandatory rules. The Chapter notes that binding rules will be appropriate where it is necessary to supplement the UPPs with higher or more prescriptive standards. The ALRC proposes that where 'guidelines' are binding they should be renamed 'rules'.[36]

58.36 The ALRC notes that stakeholders did not raise concerns about the fact that the Section 95 and 95A Guidelines are binding. The ALRC is of the view that the proposed rules to regulate the collection, use and disclosure of personal information without consent for research under the UPPs should also be binding. It is the ALRC's intention that there be a single set of rules issued by the Privacy Commissioner in relation to the

---

35 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.
36 Proposal 44–2.

conduct of research and that these rules would replace the Section 95 and 95A Guidelines.

Proposal 58–1 The Privacy Commissioner should issue one set of rules under the proposed exceptions to the 'Collection' principle and the 'Use and Disclosure' principle in the Unified Privacy Principles (UPPs) to replace the *Guidelines Under Section 95 of the Privacy Act 1988* and the *Guidelines Approved Under Section 95A of the Privacy Act 1988.*

Research other than health and medical research

58.37 NPP 10.3 currently provides an exception for the collection of health information without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety. NPP 2.1(d) provides an exception for the use and disclosure of health information without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety. Section 95 of the *Privacy Act* provides an exception from the IPPs for acts done by agencies 'in the course of medical research'.

58.38 Despite the differences between the exceptions in the NPPs and the exception in relation to the IPPs, it is clear that the general intention is to limit the exceptions to the field of health and medical research. The OPC Review recommended that the Australian Government consider whether there was a need to permit the use and disclosure of personal information for research that does not involve health information.[37] The ALRC asked a number of questions in the Issues Paper, *Review of Privacy* (IP 31)[38] about expanding the existing exceptions to include other types of personal information or other fields of research.

58.39 The Council of Europe Committee of Ministers has recognised that the public interest in a range of research—including, but not restricted to, health and medical research—may outweigh the public interest in maintaining privacy protections:

> Any exception to that rule [that where sensitive personal information is collected for statistical purposes, it should be collected in non-identifiable form] can only be justified by major public interest, as where statistical information is needed to contain epidemics, combat the evil of drug taking, investigate the scale and pattern of sexual assaults on minors or develop aid to social groups in difficulty. Such examples, to which many more might be added, relate to matters which affect society's essential interests and in which the state has responsibilities. In such cases the guarantees on

37 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 60.

38 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 4–13, 4–32 and 8–26.

> protection of sensitive data must be adapted to the objective information needs arising from the public interest.[39]

58.40 Canadian privacy legislation allows private sector organisations to use or disclose personal information without consent where it is for 'statistical, or scholarly study or research'.[40] Canadian privacy legislation also allows public sector agencies to disclose personal information to any person or body for 'research or statistical purposes' in specified circumstances.[41]

58.41 The *Information Privacy Act 2000* (Vic) allows state agencies to use and disclose personal information where necessary for 'research, or the compilation or analysis of statistics, in the public interest'.[42] The *Personal Information Protection Act 2004* (Tas) has a similar provision.[43]

Submissions and consultations

58.42 In its submission to the Inquiry, the OPC expressed support for allowing the collection, use and disclosure of non-health information for health and medical research. This was on the basis that health and medical research may be advanced by the linking of health information with other forms of personal information. The OPC, however, did not support expanding the existing arrangements to cover other areas of research. The OPC expressed the view that the public interest in non-health and medical research was generally less compelling than the public interest in health and medical research.[44]

58.43 Where the public interest in a particular research proposal outside the health and medical field was likely to outweigh the public interest in maintaining the level of protection provided by the privacy principles, the OPC suggested that a Public Interest Determination (PID) should be sought in relation to the proposal.[45] To date, two such PIDs have been granted by the Privacy Commissioner:

- PID 5 Disclosure of personal information contained in homicide files in the ACT to the Australian Institute of Criminology for research purposes;[46] and

- PID 8 Disclosure of personal information contained in certain Commonwealth Director of Public Prosecution files that relate to serious incidences of fraud,

---

39 Council of Europe—Committee of Ministers, *Explanatory Memorandum to Recommendation No R(97)18 of the Committee of Ministers to Member States Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes* (1997), [85(b)].

40 *Personal Information Protection and Electronic Documents Act 2000* SC 2000, c 5 (Canada) ss 7(2)(c); 7(3)(f).

41 *Privacy Act* RS 1985, c P-21 (Canada) s 8(j).

42 *Information Privacy Act 2000* (Vic) sch 1 IPP 2(c).

43 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).

44 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

45 Ibid.

46 Privacy Commissioner, *Public Interest Determination 5*, effective 14 December 1991.

> dishonesty and deception to the Australian Institute of Criminology for research purposes.[47]

58.44 There was strong support among other stakeholders, however, for expanding the *Privacy Act* arrangements to include other fields of research so long as safeguards, similar to those currently in place in relation to health and medical research, were applied.[48]

58.45 The Australian Bureau of Statistics (ABS) noted that:

> More generally, through its work on health and social statistics, the ABS is aware that the community expects its information to be used effectively both at the point of service provision for the individual, and also in research for the public good. In balancing privacy against public benefit of research, there is a need to recognise this broad, but not necessarily vocal, community support for using information to achieve better social outcomes.[49]

58.46 The CSIRO noted that:

> It can be difficult at times to draw a clear line between 'health' and 'non-health' information and 'health' and 'social sciences' research. Further, researchers are increasingly seeking to integrate health and non-health personal information to facilitate the answering of more complex questions. For example, health and education experiences are fundamental to the outcomes of children and youth—in combination rather than separately …
>
> We believe that extending the federal privacy principles to allow agencies and organisations to collect non-health related sensitive information for purposes including research and statistics is highly desirable. This is because researchers are seeking to address increasingly complex questions involving health and lifestyle information, for example to determine how environmental factors influence genetic predisposition to disease.[50]

58.47 The Western Australian Department of Health also expressed the view that it is often difficult to distinguish health and medical research from other research and that social indicators are increasingly being used to understand health outcomes.[51] The

---

47 Privacy Commissioner, *Public Interest Determination 8*, effective 26 August 2002.

48 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007; Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007; Government of South Australia, *Submission PR 187,* 12 February 2007; CSIRO, *Submission PR 176,* 6 February 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; AAMI, *Submission PR 147,* 29 January 2007; Confidential, *Submission PR 143,* 24 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Insolvency and Trustee Service Australia, *Submission PR 123,* 15 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

49 Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

50 CSIRO, *Submission PR 176,* 6 February 2007.

51 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

Australian Federal Police (AFP) pointed to the importance of research in the criminal justice field and noted that PID 5 provided an example of this.[52]

58.48 The Government of South Australia expressed support for expanding the arrangements to include social science research, as well as criminological research:

> Social science research on key social issues is of critical importance to the community. There is a growing recognition of the importance of evidence-based practice in the social services and the use of research and evaluation in improving policy and service planning. Robust research, based on quality data, is required to provide the necessary evidence and directions for dealing with significant social issues, such as child abuse, family violence or homelessness. Data held by government and NGOs can contribute to better understanding of such issues and the development of effective solutions. Whilst obtaining individuals' consent would be desirable it is often not possible, particularly from those clients who are highly transient and harder to engage, are in a non-voluntary relationship (for example, child protection) or in the case of large-scale studies (such as population-based data matching).[53]

ALRC's view

58.49 The ALRC's view is that there is no in-principle reason to limit the arrangements for research under the *Privacy Act* to health and medical research. Other areas of research, such as sociology and criminology, have a strong public interest basis because of their potential to lead to significant positive outcomes for the community. In addition, the ALRC notes comments from several stakeholders that research is becoming increasing multi-disciplinary, that non-health information is often crucial to health and medical research and that, in any event, it is sometimes difficult to define what amounts to health and medical research and what does not.

58.50 The ALRC notes that the National Statement and its oversight mechanisms, including review by HRECs, is designed to cover all human research, that is, research 'conducted with or about people, or their data or tissue'. The existing regime in relation to health and medical research under the *Privacy Act* relies to a certain extent on the safeguards provided by the National Statement and, in particular, on review of research proposals by HRECs. Those safeguards also can be applied to research more generally.

58.51 In addition, the *Privacy Act*, itself, can and should include a range of limits and safeguards to ensure that personal information is only used without consent for research purposes in appropriate circumstances, for example: where the research cannot be undertaken using personal information that does not identify individuals; it is impracticable to seek individuals' consent to the collection, use or disclosure of their information; and the research is conducted in accordance with rules issued by the Privacy Commissioner. These safeguards are discussed in more detail below.

---

52 Australian Federal Police, *Submission PR 186,* 9 February 2007.

53 Government of South Australia, *Submission PR 187,* 12 February 2007.

58.52 The ALRC proposes, therefore, that the *Privacy Act* be amended to extend the arrangements relating to the collection, use and disclosure of personal or health information in health and medical research to include the collection, use and disclosure of personal information in human research more generally.

Proposal 58–2 The *Privacy Act* should be amended to extend the existing arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

Definition of research

58.53 Given this proposed expansion of the arrangements relating to research under the *Privacy Act*, it is necessary to consider defining the term 'research' for the purposes the Act. Section 6 of the *Privacy Act* currently states that '*medical research* includes epidemiological research', but the term is not otherwise defined.

58.54 The IPPs do not refer to health or medical research, but s 95 of the *Privacy Act*[54]—which establishes the research exception under the IPPs and provides for the development of the Section 95 Guidelines—refers to 'medical research'. The NPPs refer to research, or the compilation or analysis of statistics, relevant to public health or public safety. It is therefore necessary to show that research or the compilation or analysis of statistics is relevant to public health or public safety to bring the activity within the existing regime established by the NPPs and the Section 95A Guidelines. The NHMRC has expressed the view that there is no obvious rationale for the differences between the approach to research taken by s 95 of the *Privacy Act* and the NPPs.[55]

58.55 The National Statement makes the point that

> There is no generally agreed definition of research; however, it is widely understood to include at least investigation undertaken to gain knowledge and understanding or to train researchers.[56]

---

54 Section 73 of the *Privacy Act*, which deals with applications for Public Interest Determinations by the NHMRC, also refers to 'medical research'.

55 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

56 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 7.

58.56 Rather than attempting to define 'research', the National Statement adopts a contextual approach. It attempts to define those activities that should fall under the National Statement, by asking the following two questions:

- What is *human* research?
- When and by what means does human research, or other activities such as quality assurance or improvement, or clinical audit, need ethical review?

58.57 As noted above, human research is defined broadly in the National Statement as research 'conducted with or about people, or their data or tissue'. The National Statement then sets out the circumstances in which such research requires ethical review:

> Research with more than a low level of risk (as defined in paragraph 2.1.6, page 18) must be reviewed by an HREC. Research involving no more than low risk may be reviewed under other processes described in paragraphs 5.1.18 to 5.1.21 (page 79). Institutions may also determine that some human research is exempt from ethical review (see paragraphs 5.1.22 and 5.1.23, page 79).[57]

58.58 Risk is defined as potential for harm, discomfort or inconvenience and involves:

- the likelihood that a harm (or discomfort or inconvenience) will occur; and
- the severity of the harm, including its consequences.[58]

Submissions and consultations

58.59 DOHA noted in relation to the draft *National Health Privacy Code*[59] that:

> In relation to the definition of the term 'research', as outlined above the approach taken in NHPP 1 of the draft Code was to leave the term undefined, but to refer to the activities of 'research or the compilation or analysis of statistics'. There is room within the guidelines designed to support the application of this principle, to provide guidance on the meaning of the term 'research'. Such an approach would appear to be appropriate and effective.[60]

58.60 The OPC also expressed the view that the *Privacy Act* should not attempt to define the term 'research'.[61]

---

57 Ibid, 8.
58 Ibid, 15.
59 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003).
60 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.
61 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

58.61 Some stakeholders, however, felt it was important to include a definition.[62] Others expressed support for the approach adopted in the National Statement.[63] The NHMRC was also of this view, noting that there was no obvious rationale for the differences in the IPPs and the NPPs and that there is very worthwhile research occurring in the health and medical sector that may not fit within the current descriptions of 'medical research' or 'research … relevant to public health or public safety'.[64] The Office of the Health Services Commissioner in Victoria expressed the view that any definition should be consistent with the National Statement as the recent review and redrafting of that document had been a very thorough process.[65]

58.62 The Western Australian Department of Health expressed the view that the principle purpose of defining the term research in the *Privacy Act* would be to distinguish those activities that must be given independent review by an HREC.[66]

ALRC's view

58.63 The ALRC's view is that the term 'research' in the *Privacy Act* should not be defined except by reference to the National Statement. The existing regime in relation to health and medical research under the *Privacy Act* and the Section 95 and 95A Guidelines relies on safeguards set out in the National Statement and, in particular, on review of research proposals by HRECs. The ALRC proposes, above, to extend the arrangements relating to the use of personal information in health and medical research to include the use of personal information in research involving humans more generally. The ALRC agrees with stakeholders that, because the proposed research regime to be established under the *Privacy Act* will continue to rely on review by HRECs, it will be important to ensure that research covered by the *Privacy Act* exceptions falls comfortably within the limits of research activities subject to review by HRECs under the National Statement. The role of HRECs in this process is discussed further, below.

58.64 Currently the NPPs refer to research or the compilation or analysis of statistics. The National Statement does not refer to the compilation or analysis of statistics but HRECs are asked to review research proposals consisting of the compilation or analysis of statistics or including statistical elements. It is possible to argue that the term 'research' is broad enough to include the compilation or analysis of statistics but this is not universally accepted. In order to put the matter beyond doubt for the

---

62 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

63 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006.

64 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

65 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

66 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

purposes of the *Privacy Act*, the ALRC proposes the Act should expressly state that the term 'research' includes 'the compilation and analysis of statistics'.

58.65 Finally, and as discussed in Chapter 57, the ALRC notes that some funding, management, planning, monitoring, improvement and evaluation of health service activity may also be characterised as research. Where particular activities can be characterised as both management activities and research the ALRC is of the view that the activity should be conducted in accordance with the proposed rules issued by the Privacy Commissioner in relation to management activities and should also be subject to the provisions relating to research, including review by an HREC.

Proposal 58–3 The *Privacy Act* should be amended to provide that 'research' is any activity, including the compilation or analysis of statistics, subject to review by a Human Research Ethics Committee under the *National Statement on Ethical Conduct in Human Research* (2007).

The public interest balance

58.66 In the second reading speech for the Privacy Amendment (Private Sector) Bill, the then Attorney-General, the Hon Daryl Williams AM QC MP, stated that:

> The balance between the interests of privacy and the need to facilitate medical research was an issue that the Privacy Commissioner and the government looked at closely. The bill provides that, where information is collected for research purposes, it must be collected with consent or, where this is not practicable, in accordance with strict safeguards set out in the bill. In addition, researchers must take reasonable steps to de-identify personal information before the results of research can be disclosed.[67]

58.67 As noted above, the *Privacy Act* requires the Privacy Commissioner to be satisfied before approving guidelines under ss 95 or 95A that the public interest in the relevant research outweighs to a substantial degree the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs.

58.68 The Section 95 and 95A Guidelines include a similar public interest test. Where research may breach the IPPs or NPPs, the Guidelines provide that the research must be approved by an HREC. Before approving a particular research proposal under the Guidelines, HRECs are required to consider whether the public interest in the research substantially outweighs the public interest in the protection of privacy.[68] In considering the public interest balance, HRECs are required to consider certain specified matters including:

---

67 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).

68 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), Guideline 3.2; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), Guideline D.4.

- the value and public importance of the research;
- the likely benefits to the participants;
- whether the research design can be modified;
- the financial costs of not proceeding with the research;
- the type of personal information being sought;
- the risk of harm to individuals; and
- the extent of a possible breach of privacy.

58.69 A number of the submissions to the OPC Review expressed the view that the *Privacy Act* and the Section 95 and 95A Guidelines fail to achieve an appropriate public interest balance. In his submission—the text of an address to the Australian Epidemiological Association—Dr Richie Gun of the Department of Public Health, University of Adelaide, discussed the particular difficulties faced by epidemiologists, and the problems he has faced in gaining access to data in cancer registries. He states that:

> In Australia we are now in a uniquely advantageous position to carry out such research, as we have mandatory registration of cancers in every State and Territory. We therefore have almost complete enumeration of all invasive cancers occurring in Australia, with the potential to carry out epidemiological studies on cancer incidence equal to or better than anywhere else in the world. Unfortunately privacy laws are impeding access to cancer registry data, so that it is becoming increasingly hard to carry out the linkage of cancer registrations with exposure data.[69]

58.70 The OPC Review stated that:

> There is considerable evidence that key researchers, especially epidemiological researchers, consider that the current balance between privacy and the public benefit of research is too heavily weighted in favour of individual privacy to the detriment of research. By gaining access to population data and data linkage, the research might considerably benefit disadvantaged groups that are currently under researched.[70]

58.71 The OPC Review noted that consumer research on attitudes in this area have produced mixed results. Research conducted by the OPC indicated that individuals were concerned about their personal information being used, even in a de-identified form, for research purposes. Almost two thirds (64%) of respondents felt that consent

---

69 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

70 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

should be obtained before de-identified information derived from personal information was used for research purposes. One third (33%) of respondents felt that permission was not necessary.[71]

58.72 The Australian Consumers' Association, in its submission to the OPC Review, expressed the view that when consumers go to the doctor, they provide health information on the basis that it will be used only for the purposes of their clinical care:

> They don't expect that third parties will be trawling through their health records; even if it is in de-identified form. In this sense third party access to data without the consumers' knowledge is something of a breach of trust.[72]

58.73 On the other hand, DOHA research suggests that, although consumers express strong reservations about identified personal information being made available for purposes other than their own clinical care, they are generally very accepting of the notion of sharing de-identified health information amongst health planners and researchers.[73] Research conducted by the NHMRC indicated that there was considerable support among the general public (66%) and health consumers (64%) for approved researchers to match information from different databases. There was an even higher level of support for approved researchers to access health information from databases where health information was identified by a unique number rather than a name.[74]

58.74 A number of submissions to the OPC Review noted that the issue of consumer support could be addressed by greater efforts to increase public awareness and acceptance of the use of health information for research, and in particular epidemiological research. Such efforts could include the publishing of research findings and public health outcomes in the popular media, and holding forums that highlight the need for this kind of research.[75] It would also be possible to raise awareness about the application of the *Privacy Act* in the research context.

58.75 The OPC Review recommended that:

> As part of a broader inquiry into the Privacy Act (see recommendation 1), the Australian Government should consider … where the balance lies between the public interest in comprehensive research that provides overall benefits to the community,

---

71 Ibid, 211.

72 Australian Consumers Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 October 2004.

73 Australian Government Department of Health and Ageing, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

74 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

75 Australasian Epidemiology Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004; Telethon Institute for Child Health Research, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

> and the public interest in protecting individuals' privacy (including individuals having choices about the use of their information for such research purposes).[76]

Submissions and consultations

58.76 In its submission to the Inquiry, the OPC expressed the view that the current public interest test was appropriate, that is, where research proposes to use identifiable personal or health information without consent, the public interest in the research must substantially outweigh the public interest in the protection of privacy. The OPC noted that, in general

> individuals expect to be given the opportunity to consent to the handling of their health information for research purposes. The section 95 and 95A mechanisms provide a way of ensuring that important health and medical research can be undertaken in circumstances where the community's expectations around consent cannot be met. The mechanisms provide a sound framework of accountability and oversight of the handling of health information without consent.[77]

58.77 The OPC also noted that

> privacy safeguards are necessary for research to remain effective. If individuals do not feel that their personal information is going to be appropriately protected, they may avoid treatment, or may supply partial or inaccurate information to the detriment of their clinical well-being and the ultimate quality of any research which may utilise their health information.[78]

58.78 In its submission to the Inquiry, DOHA stated that:

> The Department considers that the appropriate test for a HREC, considering a research proposal, is that the Committee must be satisfied that the public interest in the proposed activity 'substantially outweighs' the public interest in the protection of privacy ... Health information collected in the delivery of healthcare services is subject to a legal duty of confidence. In order to comply with this duty, express consent would normally be required before health information was disclosed for research purposes. It would not appear sufficient to discharge this duty by 'finely' balancing the public interests. The balance should be 'clearly' in favour of the research.[79]

58.79 A number of other stakeholders also expressed support for maintaining the current public interest test.[80]

---

76 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 60.

77 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

78 Ibid.

79 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

80 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

58.80 On the other hand, there was also support for modifying the test.[81] The Office of the Health Services Commissioner in Victoria stated that the "current definition with the use of the words 'substantially outweighs' has lead to ethics committees taking an overly conservative approach" and suggested that the approach adopted in the draft *National Health Privacy Code* would be more appropriate.[82] NHPP 1 of the draft Code provides that research must be in the public interest in order for it to proceed, but that it must proceed in accordance with rules issued for the purpose.

58.81 The NHMRC was very clearly of the view that

> the current requirement in the *Privacy Act* and the Section 95 and Section 95A Guidelines that the public interest in research 'substantially outweighs' or 'outweighs to a substantial degree' the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs is unbalanced and is limiting the conduct of important health and medical research …
>
> In undertaking an assessment for the purposes of determining the balance of public interests, an HREC routinely assesses a range of issues, which are detailed in the Issues Paper. This assessment provides a robust framework and in our view protects the reasonable interests of individuals. It is clear that an assessment would not favour research that has the potential to cause significant harm to individuals.
>
> We consider that a more appropriate and effective test that would accord with community sentiment would simply be that the balance of public interests favours the research proceeding.[83]

58.82 In response, the OPC expressed the view that the difficulty for researchers was not the current public interest test but rather that the

> difficulties reported by the researchers arise from the complexity of interactions between national and state legislation, the complexity of HREC processes and possibly a need for additional education within the research community about working within the privacy framework. It has also been suggested that uncertainty introduced by the complexity of the section 95 and 95A mechanisms may result in HREC's being somewhat over cautious in their approval of research proposals. These difficulties do not result from an imbalance embedded within the *Privacy Act* itself.[84]

ALRC's view

58.83 The ALRC agrees with the OPC that other elements of the current regime regulating the use of personal information in the research context also give rise to difficulty and some confusion. These issues are addressed by other proposals in this Discussion Paper including the proposals in Chapter 4 aimed at national consistency and Proposal 15–2 on the establishment of a single set of Unified Privacy Principles.

---

81 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006.

82 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007.

83 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

84 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

58.84 Currently ss 95 and 95A of the *Privacy Act* require that the Privacy Commissioner must not approve guidelines issued under these sections unless the Commissioner is satisfied that the public interest in research outweighs to a substantial degree the public interest in maintaining adherence to the IPPs or the NPPs. The ALRC is of the view that there is a demonstrable public interest in allowing some research involving the collection, use and disclosure of personal information without consent to proceed and that this is a matter for the Australian Parliament to consider in deciding whether to establish an exception to the UPPs for research. It is unnecessary for the Privacy Commissioner to consider this issue before approving guidelines or, in the ALRC's proposed regime, issuing rules. Instead, the balance of the public interest needs to be considered by an HREC in relation to each individual research proposal within the framework established by the Australian Parliament in the *Privacy Act*.

58.85 As to the test itself, the ALRC is concerned that the current test may be leading to overly conservative decision making by HRECs that is not in the overall public interest. If the public interest in a particular research proposal going forward outweighs the public interest in maintaining the level of privacy protection provided by the privacy principles, then there is an argument that the research should be allowed to proceed.

58.86 In considering this issue, it is important to keep in mind the other limits and safeguards that apply to research using personal information without consent under the *Privacy Act* and the Section 95 and 95A Guidelines. For example, HRECs must consider whether the research could proceed using information that does not identify individuals including the impact this would have on the research and the cost implications. If the researcher can establish that it is necessary to use identified personal information, issues HRECs are required to consider include: whether access to the information is restricted to appropriate personnel involved in the research; the procedures in place to ensure that personal information is permanently de-identified before the publication of results; and the procedures in place to ensure the security of the information and when it will be destroyed or returned to the original data custodian.[85] In addition, it must be impracticable for the researcher to seek consent from individuals to use their information. 'Impracticable to seek consent' is discussed further below, but must involve concrete and substantial obstacles, as opposed to mere inconvenience.

58.87 The ALRC has carefully considered the divergent views on this important issue. Chapter 1 examines the right to privacy in some detail and notes that the right is not absolute. The public interest in protecting this private right must be considered in the context of other rights and other public interests. The ALRC's view is that it is not the

---

85 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), 3.3; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), D.5.

degree to which one public interest outweighs another—whether slightly or substantially—that should be at issue. If, taking all relevant factors into account, the public interest in one course of action outweighs the public interest in another course of action, the ALRC is of the view that the appropriate course of action is clear.

58.88 The ALRC has proposed above that the areas of research and the kinds of personal information available to researchers should be broadened. The ALRC is of the view that the public interest test should be the same for all human research.

58.89 Proposals 58–8 and 58–9, below, set out proposed research exceptions to the 'Collection' and 'Use and Disclosure' principles in the UPPs. These exceptions require an HREC to review research that proposes to collect sensitive information without consent, or to use or disclose personal information without consent and be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs. The Section 95 and 95A Guidelines include guidance for HRECs in considering the balance of public interests. The ALRC is of the view that the rules to be issued by the Privacy Commissioner under the research exceptions should also address this issue.

Proposal 58–4 The research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle should provide that before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.

Impracticable to seek consent

58.90 NPP 10 and NPP 2 allow the collection, use and disclosure of health information for research without consent where it is *impracticable* for the organisation to seek the individual's consent before the collection, use or disclosure. The Section 95 Guidelines allow the collection, use or disclosure of personal information by agencies without consent when it is reasonable for the research to proceed without this consent.[86]

58.91 The 1999 National Statement provided that an HREC may approve access to data without consent where it was satisfied that: it was impossible in practice, due to the quantity, age or accessibility of the records to be studied to obtain consent, or the procedures required to obtain consent were likely either to cause unnecessary anxiety for those whose consent would be sought or to prejudice the scientific value of the

86 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.2(a)].

research; and the public interest in the research outweighed to a substantial degree the public interest in privacy.[87]

58.92 In its submission to the OPC Review, the NHMRC expressed the view that the consent provisions of the National Statement and the *Privacy Act* should be consistent. The *Privacy Act* regime should allow the use and disclosure of health information in health and medical research where seeking consent may prejudice the scientific value of the research, or where the procedures necessary to obtain consent are likely seriously and adversely to affect the well being, including the psychological health, of the individual.[88] A number of other submissions to the OPC Review expressed the view that the circumstances in which the NPPs allow the collection, use and disclosure of health information without consent are too narrow.[89]

58.93 In ALRC 96, the ALRC and AHEC recommended that:

> The NHMRC, as part of its review of the National Statement in the 2003–2005 triennium, should ensure that the provisions of the National Statement relating to waiver of consent and reporting of decisions are consistent with privacy laws and, in particular, with guidelines issued under s 95 and s 95A of the *Privacy Act 1988* (Cth).[90]

58.94 The 1999 *National Statement on the Ethical Conduct in Research Involving Humans*, to which this recommendation relates, has been revised and redrafted following extensive consultation and debate. The 2007 *National Statement on Ethical Conduct in Human Research*[91] provides detailed provisions relating to consent, including provisions dealing with the qualifying or waiving of consent requirements in some circumstances. The revised National Statement makes clear that HRECs or other ethical review bodies may waive the requirement for consent if satisfied that:

> (a) involvement in the research carries no more than low risk (see paragraphs 2.1.6 and 2.1.7, page 18) to participants;
>
> (b) the benefits from the research justify any risks of harm associated with not seeking consent;

---

87 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), [14.4].

88 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

89 Australian Compliance Institute Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004; University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004; Australasian Epidemiology Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004.

90 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 15–2.

91 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

> (c) it is impracticable to obtain consent (for example, due to the quantity, age or accessibility of records);
>
> (d) there is no known or likely reason for thinking that participants would not have consented if they had been asked;
>
> (e) there is sufficient protection of their privacy;
>
> (f) there is an adequate plan to protect the confidentiality of data;
>
> (g) in case the results have significance for the participants' welfare there is, where practicable, a plan for making information arising from the research available to them (for example, via a disease-specific website or regional news media);
>
> (h) the possibility of commercial exploitation of derivatives of the data or tissue will not deprive the participants of any financial benefits to which they would be entitled;
>
> (i) the waiver is not prohibited by State, federal, or international law.[92]

Submissions and consultations

58.95 In its submission to the inquiry the CSIRO noted that:

> Some investigations have been done on the possibility that consent processes may lead to bias in the makeup of study groups, and that this in turn may jeopardise the quality of the results.[93]

58.96 The OPC Review also noted evidence that requiring consent to participate in some research projects significantly reduces the participation rate—and therefore the scientific value and integrity of the research.[94]

58.97 A number of stakeholders expressed support for the existing framework providing for the use of personal information in research where obtaining consent is impracticable.[95] The Australian Nursing Federation expressed the view that the framework was appropriate but that further guidance was needed as to the meaning of 'impracticable'.[96] A number of stakeholders expressed support for the proposition that the *Privacy Act* and the National Statement should be consistent.[97]

58.98 One stakeholder felt that 'impracticable' was too vague and set the bar too low.[98] The NSW Council for Civil Liberties expressed the view that where information

---

92 Ibid, Ch 2.3.
93 CSIRO, *Submission PR 176,* 6 February 2007.
94 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.
95 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
96 Australian Nursing Federation, *Submission PR 205,* 22 February 2007.
97 Ibid; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.
98 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

was to be used without consent this should be approved by the Privacy Commissioner, as well as by an HREC.[99]

58.99 The NHMRC expressed the view that:

> The NHMRC considers that impracticability of consent is one of many criteria that should be considered when an assessment is being made of the balance of public interests in the collection, use or disclosure of personal information without consent for research purposes. Given the large number of criteria, including impracticability of consent, that need to be assessed to determine the balance of public interests, we propose that specific reference to 'impracticability of consent' as a precondition to referral for consideration under the Research Guidelines is removed from the NPPs but continues to be incorporated into the associated Research Guidelines as one of the important criteria to be assessed. The criteria detailed in the Research Guidelines for assessment of the balance of public interests generally should reflect those included in the draft *National Statement*.[100]

58.100 In its submission, the OPC expressed the view that the framework contained in the NPPs for the use of health information in research without consent is appropriate and effective and did not support amendments in this area. The OPC noted that whether it is impracticable to seek consent depends on the particular circumstances of the case, and that the OPC has issued guidance on the issue.[101] The OPC is of the view that researchers are required to take reasonable steps to seek consent. There must be compelling justification to support the collection, use or disclosure of health information without consent and this means concrete and substantial obstacles, as opposed to mere inconvenience.[102]

58.101 The OPC provided the following examples of situations that might give rise to impracticality for the purposes of the *Privacy Act*:

- individuals may be uncontactable due to death or relocation (this particularly arises in relation to old records);
- individuals of interest may be part of a demographic group that is difficult to contact (for example, remote/indigenous groups);
- the number of records involved may cause logistical problems; or

---

99 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.
100 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
101 Office of the Federal Privacy Commissioner, *Handling Health Information for Research and Management*, Information Sheet 9 (2001).
102 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

- the objective of the investigation may need to be concealed from subjects in order to minimize various forms of bias. For example, having to obtain consent in blind trials could compromise the integrity of the research.[103]

58.102 The OPC also commented that:

> Organisations suggesting that consent is impracticable on the grounds that it would invalidate the research methodology should consider if this is the conclusion that a reasonable person, independent of the research project, would come to. As the Office stated in its Information Sheet on the subject, 'Impracticability' should be something more than incurring some expense or effort in seeking an individual's consent.[104]

ALRC's view

58.103 The ALRC has formed the view that, although there is room for interpretation in regard to what amounts to 'impracticable' to seek consent, it is an appropriate element of the framework permitting the use of personal information without consent for research. It provides a flexible test that can be applied in a variety of situations. The ALRC's view is that it does not set the bar too low. Impracticable means 'more than incurring some expense or effort in seeking an individual's consent'. The obstacles to seeking consent must be real and they must be significant.

58.104 The ALRC agrees with stakeholders that it is important to maintain a certain level of consistency between the *Privacy Act* and the National Statement. The ALRC notes that the revised National Statement includes 'impracticable to obtain consent' as one of the criteria an HREC or other review body must consider in determining whether to grant waiver of consent to use personal information in research.[105] The ALRC is not concerned that the National Statement also includes other criteria in this list. The *Privacy Act* provides preliminary criteria that must be satisfied before a research proposal can proceed without consent, and the National Statement provides a more detailed list of matters HRECs and other review bodies must consider in deciding whether to allow a proposal to proceed without consent. This approach is not incompatible with the *Privacy Act*.

58.105 The proposed research exception to the UPPs, discussed below, retains the requirement that it must be impracticable for an agency or organisation to seek the individual's consent to the collection, use or disclosure of personal information in research. The proposed exception to the UPPs also requires that an HREC be satisfied that the public interest in the collection, use or disclosure outweighs the public interest in maintaining the level of privacy protection provided by the UPPs. The criteria set out in the National Statement are relevant to this decision on the balance of public interests.

---

103 Ibid.

104 Ibid.

105 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [2.3.6(c)].

58.106 The proposed research exception to the UPPs also requires that any such research is conducted in accordance with rules issued by the Privacy Commissioner. It is expected that the Privacy Commissioner will develop these rules in consultation with stakeholders, including the authors of the National Statement: the NHMRC, the Australian Research Council and the AVCC. This will provide an opportunity to ensure that the framework established under the *Privacy Act* to allow research that is in the public interest to proceed without consent is consistent with the framework established by the National Statement to allow HRECs and other review bodies to grant waiver of consent for such research.

Proposal 58–5 The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, to ensure that the approaches adopted in the rules and the *National Statement on Ethical Conduct in Human Research* (2007) are compatible.

Human Research Ethics Committees

58.107 Institutions that undertake research 'with or about people, their data or tissue'[106] are responsible for ensuring that research they conduct, or for which they are responsible, is ethically reviewed in accordance with the National Statement.[107] Institutions may establish their own processes for ethical review or use those of another institution.[108]

58.108 The National Statement provides that ethical review can be undertaken at various levels depending on the degree of risk involved in the research. Research involving 'negligible risk' and the use of existing collections of data or records that contain only non-identifiable information may be exempt from review.[109] Research involving 'no more than a low level of risk' may be reviewed by a non-HREC ethical review body.[110] Non-HREC ethical review includes review by a head of department, a departmental committee, or a subcommittee of an HREC.[111] Research involving more than a low level of risk must be reviewed by an HREC. The National Statement expressly provides that research proposing to use personal information in medical research without consent and research using health information without consent must

106 Ibid, 8. This is the definition of 'human research' used in the National Statement.
107 Ibid, [5.1.1].
108 Ibid, [5.1.3].
109 Ibid, [5.1.22].
110 Ibid, [5.1.7].
111 Ibid, [5.1.20].

be reviewed by an HREC.[112] These provisions reflect the existing exceptions for research under the IPPs and NPPs.

58.109 HRECs must be composed and function in accordance with the National Statement.[113] The minimum membership of an HREC is eight: a chairperson; at least two lay people (one man and one woman) who have no affiliation with the institution; at least one person with knowledge of and experience in the professional care, counselling or treatment of people; at least one person who performs a pastoral care role in the community; at least one lawyer; and at least two people with current research experience.[114] The primary responsibility of HREC members is to decide whether a proposal meets the requirements of the National Statement and is ethically acceptable.[115]

58.110 Both the Section 95 and 95A Guidelines provide a detailed framework within which HRECs must consider the privacy implications of research proposals involving the use of individuals' personal or health information. In particular, HRECs must consider, and may approve, research proposals seeking to use personal or health information without consent, on the basis that the public interest in the research substantially outweighs the public interest in maintaining the level of privacy protection provided by the IPPs and the NPPs.

58.111 The Guidelines require that, before making a decision, an HREC must assess whether it has sufficient information, expertise and understanding of privacy issues, either amongst the members of the HREC or otherwise available to it, to make a decision that takes proper account of privacy.[116] The Section 95A Guidelines note that it may be necessary to appoint additional members with specific expertise in some circumstances. It is important to note that, although an HREC may give approval for a research proposal to proceed, the final decision to release personal information to researchers is not made by an HREC but by the relevant data custodian.

58.112 The Guidelines also require HRECs to record their decisions, including details of the agency or organisation from which information will be sought, the information sought, the number of records involved, and the IPP or NPP likely to be infringed.[117] AHEC is in turn required to report annually to the NHMRC in relation to HRECs generally, and to provide a compliance report setting out decisions taken by

---

112 Ibid, [2.3.5].
113 Ibid, Ch 5.1.
114 Ibid, [5.1.30].
115 Ibid, [5.2.2].
116 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [D.1].
117 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [3.4]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [D.6].

HRECs under the Guidelines.[118] AHEC is also required to provide the compliance report to the Privacy Commissioner[119] and to report where there has been a breach of the Guidelines.[120]

58.113 Submissions to the OPC Review suggested that the reporting obligations imposed on HRECs by the guidelines are detailed and unnecessarily onerous, for example, the requirement to list those IPPs and NPPs that may be breached by the research proposal.[121] The OPC Review considered this issue and made the following recommendation:

> The Office will work with the National Health and Medical Research Council to simplify the reporting process for human research ethics committees under the section 95A guidelines.[122]

58.114 A number of other issues were identified in the course of the OPC Review, including the tendency of HRECs to make conservative decisions, refusing access to health information if there is any risk of being in breach of the law; and the need to involve a number of HRECs in decision making in relation to research proposals, particularly national proposals.[123] Concern was also expressed about inconsistencies in the way HRECs balance the public interests in research and privacy,[124] and in relation to membership of HRECs.[125] Similar issues were raised in the course of the current Inquiry.[126]

58.115 In ALRC 96, the role and function of HRECs in the context of genetic research was considered in detail, and a range of recommendations to improve HREC

---

118 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [4.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [E.1].

119 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [5.1]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [F.1].

120 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), [4.3]; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), [E.3].

121 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004; University of Western Australia Human Research Ethics Committee, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004.

122 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 62.

123 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

124 South Australian Government Department of Health, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

125 University of Adelaide, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004.

126 B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006.

decision making and to support HRECs in their work were made. In particular, Recommendation 17–1 states that:

> The National Health and Medical Research Council (NHMRC) should develop and implement procedures to promote consistency, efficiency, transparency and accountability in the review of human genetic research by Human Research Ethics Committees (HRECs). In developing such procedures, the NHMRC should initiate a systematic quality improvement program that addresses:
>
> - consolidation of ethical review by region or subject-matter;
> - the membership of HRECs and, in particular, the balance between institutional and non-institutional members;
> - the need for expertise of HRECs in considering proposals for human genetic research;
> - on-going monitoring of approved human genetic research projects;
> - the education and training of HREC members;
> - payment of HREC members for their work in reviewing research proposals;
> - independent audit of HREC processes; and
> - standardised record keeping and reporting to the NHMRC, including in relation to commercial arrangements.[127]

58.116 The ALRC and AHEC also recommended that:

> The NHMRC, in strengthening the level of training and other support provided to HRECs in accordance with Chapter 17 of this Report, should ensure that adequate attention is given to: (a) the interpretation of the waiver of consent provisions of the National Statement; and (b) HREC decision making in relation to such waiver.[128]

58.117 A number of initiatives are under way to address these issues. In particular, the CSIRO noted in its submission that:

> At the October 2006 meeting of the Australian Health Ministers Advisory Council, agreement was reached on establishing a nationally harmonised system of scientific and ethics review of multi-centre health and medical research. The national coordinating body will be the NHMRC, which is tasked with creating a national harmonized system based on mutual recognition by all jurisdictions of the single review undertaken by recognised human research ethics committees in any jurisdiction …
>
> A key development in removing impediments to such multi-centre research has been the National Ethics Application Form (NEAF)13, available for public use since May 2006. This Application Form is an electronic, web based form for use by researchers

---

127 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 17–1.

128 Ibid, Rec 15–3.

> in any research discipline when submitting research proposals to one or more Human Research Ethics Committee (HREC) for review.[129]

58.118 The NHMRC was awarded $5.6 million in the 2007 federal budget to establish a national system for single ethical review of cross-jurisdictional and multi-centre research by establishing national committees to conduct a single review of such research.[130] In addition, the National Statement has been extensively revised and redrafted.[131] The New South Wales Department of Health has developed its own model of single ethical review of multi-centre research in the New South Wales public sector. The model was implemented on 1 July 2007.[132] The Victorian Government Department of Human Services is also working on a project to implement a centralised system of ethical review for multi-centre research.[133]

58.119 Given these recent comprehensive reviews and developments, the ALRC does not propose to reconsider the HREC decision-making process in detail. In IP 31, however, the ALRC asked whether HRECs are the most appropriate bodies to make decisions about the collection, use and disclosure of personal information without consent in the context of health and medical research. In addition, the ALRC asked whether the requirements imposed on HRECs by the Section 95 and 95A Guidelines are appropriate and effective.[134]

Submissions and consultations

58.120 In its submission to the Inquiry, the NHMRC urged

> the ALRC to reconsider the role of HRECs in decisions about the privacy implications of the collection, use or disclosure of health information in research. The NHMRC is of the view that these considerations could be managed without intervention by an HREC although we have not identified a replacement mechanism at this stage.[135]

58.121 One other stakeholder suggested that the establishment of a centralised, national approval process would improve the efficiency and consistency of decision making.[136] Having asked the ALRC to reconsider the issue, however, the NHMRC also expressed the view that HRECs are, in general, appropriately constituted to enable

---

129 CSIRO, *Submission PR 176,* 6 February 2007.

130 Australian Government Department of Health and Ageing, *Health and Medical Research—Streamlining Human Research Ethics Reviews* (2007) <www.health.gov.au/budget2007> at 27 August 2007.

131 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007).

132 New South Wales Government Department of Health, *NSW Health Model for Single Ethical and Scientific Review of Multi-Centre Research* (2007) <www.health.nsw.gov.au/healthethics/multicentre_research.html> at 27 August 2007.

133 Victorian Government Department of Human Services, *Streamlining Ethical Review of Multi-Centre Research in Victoria* (2007) <www.health.vic.gov.au/ethics/multi/index.htm> at 27 August 2007.

134 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 8–31, 8–32.

135 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

136 A Smith, *Submission PR 79,* 2 January 2007.

them to perform the role assigned to them under the *Privacy Act* and Section 95 and 95A Guidelines.

58.122 The NHMRC also expressed concern about the reporting requirements imposed on HRECs by the Section 95 and 95A Guidelines. The NHMRC noted that the complexity of the regulatory regime and the detailed reporting requirements have resulted in an excessive administrative burden associated with those responsibilities. The NHMRC suggested a reporting framework that involved less detailed, commentary-based reporting on privacy issues that arise during a reporting period, and an exception-based reporting framework for specific privacy concerns that come to the attention of HRECs during a reporting period.[137]

58.123 In its submission to the Inquiry, the OPC expressed the view that HRECs are the most appropriate bodies to make decisions about the collection, use and disclosure of health information without consent in the health and medical research context. The OPC reiterated that it would work with the NHMRC to simplify the reporting requirements under the Section 95 and 95A Guidelines.[138]

58.124 There was strong support from other stakeholders for the role of HRECs in reviewing proposals under the *Privacy Act* and the s 95 and s 95A Guidelines.[139] The Centre for Law and Genetics stated that:

> We are strongly of the view that Human Research Ethics Committees are the most appropriate bodies to make decisions about the collection, use and disclosure, without consent, of health information in the context of health and medical research. This model of ethical review, based on the collective wisdom of an interdisciplinary group, has proved in general to be very effective in practice.[140]

58.125 The Centre for Law and Genetics also expressed support for the recommendations relating to HRECs in ALRC 96.[141] The Caroline Chisholm Centre for Health Ethics noted the need for adequate funding, training and education of HRECs and their members.[142]

---

137 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

138 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

139 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007; Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Health Informatics Society of Australia, *Submission PR 196,* 16 January 2007; CSIRO, *Submission PR 176,* 6 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

140 Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

141 Ibid.

142 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

58.126 The Australian Institute of Health and Welfare (AIHW) noted that:

> The AIHW would see no difficulty with NHMRC guidelines being extended to govern use and disclosure in the broad field of health and welfare information (ie, beyond health, narrowly construed). Indeed, that is the position that the AIHW has previously put to the Privacy Commissioner and is in fact already the way that the AIHW Ethics Committee arrangements operate.[143]

ALRC's view

58.127 The ALRC has considered the role of HRECs in the privacy regime and is of the view that HRECs remain the most appropriate bodies to make decisions about the collection, use and disclosure of personal information without consent in the health and medical research context. Such review is only required when researchers propose to use identified or reasonably identifiable personal information without consent. The ALRC is of the view that this raises privacy as well as ethical issues and that such issues are appropriately considered by HRECs. The ALRC notes that there was widespread support for the role of HRECs in this area.

58.128 The National Statement and its oversight mechanisms, including review by HRECs, is not limited to health and medical research, but is intended to cover all research involving humans. The ALRC proposes, above, extending the existing arrangements relating to the collection, use and disclosure of personal information in health and medical research to include the collection, use or disclosure of personal information in research involving humans more generally. The ALRC's view is that HRECs should be required to review and approve all such activities.

58.129 The National Statement provides that only an HREC may approve research that proposes to use personal information without consent in medical research, or personal health information without consent.[144] In addition, the National Statement provides that only an HREC may approve research that involves more than a low level of risk.[145] In the context of extending the arrangements for research under the *Privacy Act*, the National Statement may also require amendment. The ALRC is of the view that any research that requires:

- the collection of identified or reasonably identifiable sensitive information without consent;
- the use or disclosure of such information without consent for a purpose that is not directly related to the purpose of collection and within the reasonable expectations of the individual; or

---

143 Australian Institute of Health and Welfare, *Submission PR 170,* 5 February 2007.

144 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [2.3.5].

145 Ibid, 8.

- the use or disclosure of identified or reasonably identifiable non-sensitive information without consent for a purpose that is not related to the purpose of collection and within the reasonable expectations of the individual,

is likely to involve more than a low level of risk for individuals and should always be reviewed by an HREC. In these circumstances, researchers will be relying on the research exceptions in the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, discussed further below. The ALRC proposes that the National Statement be amended to require that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by an HREC.

58.130 The ALRC notes developments in relation to the harmonisation and simplification of ethical review and the development of a National Ethics Application Form. In Proposal 58–1, above, the ALRC suggests that the Section 95 and 95A Guidelines be replaced by a single set of rules issued by the Privacy Commissioner. The ALRC's view is that the adoption of a single set of UPPs and a single set of rules relating to research, to be developed in consultation with stakeholders, will have a significant impact on reducing regulatory complexity and the regulatory burden on HRECs.

58.131 The development of the rules to be issued by the Privacy Commissioner in relation to research will provide an opportunity to review the reporting requirements currently imposed on HRECs and on AHEC. The ALRC's view is that any reporting requirements should have clear goals and should impose the minimum possible administrative burden to achieve those goals. This might be achieved, for example, by minimal first tier reporting of the number of proposals considered and the number approved and rejected, while allowing for follow-up by the Privacy Commissioner if these reports raised concerns or indicated undesirable trends.

Proposal 58–6 The *National Statement on Ethical Conduct in Human Research* (2007) should be amended to require that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act,* it must be reviewed and approved by a Human Research Ethics Committee.

Proposal 58–7 In developing the rules to be issued in relation to research under the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, the Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements currently imposed on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

An exception to the proposed Unified Privacy Principles

58.132 Part D of this Discussion Paper sets out a proposed set of Unified Privacy Principles. In this section the ALRC proposes exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle to allow research using identified or reasonably identifiable personal information without consent to proceed, where the public interest in allowing the research to go forward outweighs the public interest in maintaining the level of privacy protection provided by the UPPs.

58.133 Currently, NPP 10.3 provides in part that health information may be collected without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, where:

- the purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

- it is impracticable for the organisation to seek the individual's consent to the collection; and

- the information is collected as required by law; or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or in accordance with guidelines approved under s 95A.

58.134 In addition, NPP 10.4 provides that if an organisation collects health information about an individual in accordance with NPP 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

58.135 As discussed in Chapter 57, the proposed 'Collection' principle would allow the collection of sensitive information without consent where the collection is required or specifically authorised by or under law. It is not necessary, therefore, to include this element specifically in the provision dealing with collection of sensitive information without consent for research. In addition, and as discussed in Chapter 57, the OPC is not aware of any existing rules established by competent health or medical bodies that would fulfil the requirements of NPP 10.3. The ALRC, therefore, proposes to drop the references to these two mechanisms from the proposed research exception.

58.136 NPP 2.1(d) provides that an organisation may use or disclose health information without consent where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety where:

- it is impracticable for the organisation to seek the individual's consent before the use or disclosure;

- the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under s 95A for the purposes of this subparagraph; and

- in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information.

58.137 The ALRC is of the view that a similar regime should be established under the UPPs, and should apply to both agencies and organisations.

58.138 The Section 95 and 95A Guidelines are issued by the NHMRC and approved by the Privacy Commissioner. Once approved and gazetted the guidelines become binding. Because of the proposed expanded scope of the research exception, the ALRC is of the view that it is no longer appropriate to rely on the NHMRC alone to develop guidelines for the conduct of research. The ALRC proposes, therefore, that the research exception to the UPPs simply provides that the rules to guide the conduct of research should be issued by the Privacy Commissioner. The Commissioner will, of course, be free to consult with stakeholders, including the authors of the National Statement, in developing the rules. It is anticipated that the rules would address similar issues to those addressed in the existing guidelines, discussed above.

58.139 The ALRC's view is that the requirement for an HREC to review and approve research proposals, and the public interest test to be applied in that review, should be included expressly in the UPPs. Both these elements are fundamental to the exception for research and, while HRECs are currently required to review and approve research proposals seeking to rely on the research exceptions in the *Privacy Act*, the requirement for this to occur is not expressly included in the Act. Instead, it is set out in the Section 95 and 95A Guidelines.

58.140 In contrast to NPP 1, the proposed 'Collection' principle deals with the collection of both sensitive and non-sensitive information. The proposed 'Collection' principle does not require consent for the collection of non-sensitive information. Subclause 2.6 of the proposed 'Collection' principle does, however, require consent for the collection of sensitive information. Therefore, the research exception to the proposed 'Collection' principle is limited to the collection of sensitive information.

58.141 The ALRC is of the view that the wording of NPP 10.4 should be amended so that the provision no longer requires that reasonable steps be taken to 'permanently de-identify' information before it is disclosed. The ALRC's view is that it is sufficient to require agencies and organisations that collect sensitive information under the research exception to the proposed 'Collection' principle to take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable. This approach is more

consistent with the proposed definition of 'personal information' discussed in Chapter 3[146] and meets concerns raised by stakeholders, and discussed further below, in relation to the term 'de-identified'. Where information is not about an identified or reasonably identifiable individual, it will no longer fall within the definition of personal information and so will no longer covered by the *Privacy Act*.

Proposal 58–8 The research exception to the proposed 'Collection' principle should state that, despite subclause 2.6, an agency or organisation may collect sensitive information about an individual where:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

(e) the information is collected in accordance with rules issued by the Privacy Commissioner.

Where an agency or organisation collects sensitive information about an individual in accordance with this provision, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Proposal 58–9 The research exception to the proposed 'Use and Disclosure' principle should state that despite the other provisions of the Use and Disclosure principle, an agency or organisation may use or disclose personal information where:

(a) the use or disclosure is necessary for research;

(b) it is impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

146 Proposal 3–5.

(c) a Human Research Ethics Committee has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs;

(d) the information is used or disclosed in accordance with rules issued by the Privacy Commissioner; and

(e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the personal information in a form that would identify the individual or from which the individual would be reasonably identifiable.

Identifiable personal information

58.142 'Personal information' for the purposes of the *Privacy Act* is defined as

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[147]

58.143 The OPC *Guidelines on Privacy in the Private Health Sector* indicate that the *Privacy Act* does not apply to 'de-identified information or statistical data sets, which would not allow individuals to be identified'.[148] The OPC has also stated that information is de-identified when it is not possible 'to reasonably ascertain' the identity of a person from the information and that this may depend on the resources available to an organisation to re-identify the information. Whether information is de-identified so that it no longer falls within the protection of the *Privacy Act* will depend on context and circumstances.[149]

58.144 The OPC Review identified a number of problems with the concept of 'de-identified'. The NHMRC stated that stakeholders are experiencing difficulty in determining whether a person's identity is 'apparent or can be reasonably ascertained' and recommended that the OPC provide guidance on this phrase so that it is clear when information is not subject to the *Privacy Act* or the HREC approval process.[150] The AIHW also pointed to problems with determining when data is de-identified and

147 *Privacy Act 1988* (Cth) s 6.

148 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A.3.1.

149 Office of the Privacy Commissioner, 'De-identification of Personal Information', (Paper presented at Privacy Contact Officers Network Meeting, Canberra, 26 November 2004).

150 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

indicated that there is a need for more guidance.[151] The Australian Nursing Federation expressed the view that greater clarity is needed, in particular, around the de-identification of electronic data and the point at which it is adequately de-identified for the purposes of the *Privacy Act.*[152]

58.145 In response, the OPC Review stated that:

> As part of a wider inquiry into the *Privacy Act*, the issue of what is or is not de-identification could be considered. This is an important threshold issue which determines whether or not information is protected. Developments in technology have made it increasingly difficult to determine whether information is de-identified or not. In the meantime, the Office could provide guidance on this, which would help HRECs and researchers in their decision making.[153]

58.146 In Chapter 3 of this Discussion Paper, the ALRC proposes that the *Privacy Act* be amended to provide that 'personal information' is defined as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'. In addition, the ALRC considers the meaning and application of the terms 'identified' and 'reasonably identifiable' and proposes that the Privacy Commissioner issue guidance on the matter.[154] In this chapter, the ALRC considers when information has been de-identified so that it is no longer about an identified or reasonably identifiable individual. Although this issue is considered here in the context of research, the central question is of wider application, that is, does information fall within the definition of 'personal information' in the *Privacy Act.*

58.147 There is a strong public interest in the collection, use and disclosure of personal information that has been 'de-identified' for activities such as research. That is not to say that individuals have no interest in de-identified personal information about them, but that the individual's interest in the information may at some point give way to the public interest in being able to use the information freely.

58.148 A report prepared for the UK Information Commissioner notes that:

> The identity and privacy of the individual are traditionally seen as well protected by the anonymisation of personal data, thereby placing it beyond the scope of the

---

151 Australian Institute of Health and Welfare, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 23 December 2004.

152 Australian Nursing Federation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 February 2005.

153 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

154 Proposal 3–5.

> Directive as non-personal data incapable of identifying the individual subject … The broader effect of anonymisation on dignity is, however, not widely discussed.[155]

58.149 The report goes on to state that:

> 'Indirect' identification, where a person could be identified from the data or the data and other data, can only be made workable by a concept of reasonableness, as in Recital 26 [of the EU Directive], but conceptually it threatens the possibility of anonymising or pseudonymising data effectively to remove it from 'personal data'.[156]

58.150 The EU Directive states:

> Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.[157]

58.151 The NHMRC, the Australian Research Council and the AVCC have considered this issue in the context of revising the National Statement. The National Statement makes a distinction between individually identifiable data, re-identifiable data and non-identifiable data as follows:

> Data may be collected, stored or disclosed in three mutually exclusive forms:
>
> - individually identifiable data, where the identity of a specific individual can reasonably be ascertained. Examples of identifiers include the individual's name, image, date of birth or address;
> - re-identifiable data, from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets;
> - non-identifiable data, which have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. A subset of non-identifiable data are those that can be linked with other data so it can be known that they are about the same data subject, although the person's identity remains unknown.
>
> This National Statement avoids the term 'de-identified data', as its meaning is unclear. While it is sometimes used to refer to a record that cannot be linked to an individual ('non-identifiable'), it is also used to refer to a record in which identifying information has been removed but the means still exist to re-identify the individual.

---

155 S Booth and others, *What are 'Personal Data'?—A Study Conducted for the UK Information Commissioner* (2004), 8.

156 Ibid, 7.

157 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), recital 26.

> When the term 'de identified data' is used, researchers and those reviewing research need to establish precisely which of these possible meanings is intended.[158]

58.152 In IP 31, the ALRC asked whether definitions of this kind should be included in the *Privacy Act* and whether a distinction should be drawn between identifiable personal information and re-identifiable personal information in the research context.[159]

Submissions and consultations

58.153 DOHA noted the need for guidance on the meaning of terms such as 'identified', 're-identifiable', 'non-identifiable' and 'de-identified' but did not believe the terms needed to be defined in the *Privacy Act*.[160] Other stakeholders felt that definitions would be helpful, with some noting the importance of maintaining consistency with the National Statement.[161]

58.154 Some stakeholders expressed the view that no distinction should be drawn between 'identifiable' and 're-identifiable' personal information in the context of the *Privacy Act*.[162] The Australian Privacy Foundation stated that:

> Health researchers have constructed elaborate mechanisms to allow data linkage, which provide a degree of protection but do not amount to de-identification. Information either is or is not actually or potentially identifiable. The ALRC should be wary about legitimizing the idea that there can be an intermediate category.[163]

58.155 The Western Australian Department of Health expressed the view that:

> No distinction is necessary between the two categories 'identifiable' and 're-identifiable or potentially re-identifiable' data for the purposes of the *Privacy Act* since the privacy principles should apply to both.[164]

---

158 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), 29.

159 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Questions 8–27 and 8–28.

160 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.

161 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Insurance Council of Australia, *Submission PR 110,* 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006; A Smith, *Submission PR 79,* 2 January 2007 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

162 Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

163 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

164 Department of Health Western Australia, *Submission PR 139,* 23 January 2006. Other stakeholders were also of this view: Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007.

58.156 The Department went on to suggest that, in the context of the *Privacy Act*, there are only two relevant categories of personal information:

- reasonably identifiable personal information; and
- non-identifiable personal information.[165]

58.157 The Department expressed the view that 'reasonably identifiable personal information' includes information linked with an individual's name, image, date of birth or address; information that contains a unique personal identifier when the holder of the information also has the master list linking the identifiers to individuals; information that the holder can merge or link to other information they already hold, enabling them to identify individuals; and aggregated information where individuals can be identified because of the small number of individuals in particular fields of information.

58.158 The Department stated that 'non-identifiable personal information' includes information that has never been labelled with individual identifiers or from which they have been permanently removed; and information that contains a unique personal identifier where the holder cannot link the information to a specific individual because they do not hold the master list linking the identifiers to individuals.[166]

58.159 The Department also made the point that identifiability is contextual: information that is identifiable to the original holder of the information may be unidentifiable to a recipient of the information. For example, information that contains a unique personal identifier is not identifiable to a recipient who does not hold the master list. This is the basis of the data linkage protocol adopted by the Western Australian Data Linkage Unit (DLU), discussed further below. Other stakeholders agreed that the use of independent intermediaries in this way should mean that the information in the hands of data recipients is no longer classified as 're-identifiable' and, for the purposes of the *Privacy Act,* should be considered 'non-identifiable'.[167]

58.160 The Department of Human Services explained that, in deciding whether to disclose de-identified personal information to researchers, Medicare Australia carefully considered what was released in order to ensure that individuals could not be identified or re-identified. This consideration included examining what other information researchers were collecting and considering whether that information could be linked with information released by Medicare Australia in a way that would enable researchers to identify individuals.[168]

---

165 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

166 Ibid.

167 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007; Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006.

168 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

58.161 A number of other stakeholders also suggested that it was necessary to consider each disclosure on a case-by-case basis to avoid releasing information that might identify an individual, for example, because of the small number of individuals in the data set.[169] The ABS stated in its submission that:

> When the ABS publishes statistics, or releases information, it cannot do so in a manner that is likely to enable the identification of a particular person. In order to ensure the ABS complies with this requirement, the ABS has developed statistical methods to prevent the disclosure of identifiable information, while allowing sufficiently detailed information to be released to make the statistics useful.[170]

58.162 The ABS considers disclosures on a case-by-case basis and considers a range of issues, including what other information may be available to the data recipient that might allow identification through matching. The National Statistical Service Handbook, which provides guidance on these matters for Australian and state and territory government agencies notes that:

> The generation and release of statistical information from administrative record collections usually includes data that are available at a detailed level both in terms of the characteristics of individuals and their geographic location such as postcode. Although personal information such as name and address may be removed, identification of individuals may occur by putting together information already known with the data provided.
>
> The issue for agencies to address is what level of aggregation of data is required to avoid compromising the confidentiality of the individual's information and still produce meaningful data.[171]

58.163 The ABS and other agencies employ a range of techniques to minimise the risk of disclosing information that might be used to identify individuals. These include data suppression, data rounding and category collapsing. Detailed categories such as country of birth or industry or occupation can be collapsed to a less detailed level to avoid the risk of identification. Such techniques, however, can have a negative impact on the usefulness of data as some detailed data may need to be suppressed or modified.[172]

58.164 The CSIRO noted in its submission that the meaning of de-identified is often unclear. On the one hand, it may mean simply that nominated identifiers such as name, address, date of birth and Medicare number have been removed from the data. On the other hand, CSIRO refers to the extremely detailed guidance provided in s 164.[514] of

---

169 Australian Bureau of Statistics, *Consultation PC 139*, Canberra, 16 March 2007; B Armstrong, *Consultation PC 47*, Sydney, 10 January 2007; National E-Health Transition Authority, *Consultation PC 41*, Sydney, 6 December 2006.

170 Australian Bureau of Statistics, *Submission PR 96,* 15 January 2007.

171 National Statistical Service, *National Statistical Service Handbook* <www.nss.gov.au/nss/home.NSF/pages/NSS+Resources?OpenDocument> at 1 August 2007, App 4 Confidentiality and Privacy.

172 Ibid, App 4 Confidentiality and Privacy.

the *Health Insurance Portability and Accountability Act 1996* (US) (HIPA Act), which provides a number of tests to determine when health information is not 'individually identifiable health information'. The first test allows 'a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable' to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information.[173]

58.165 An alternative test in the legislation expressly sets out a long list of identifiers that must be removed to render the information not individually identifiable. The list includes: names; all geographic subdivisions smaller than a State; all elements of dates related to an individual apart from year; telephone and fax numbers; electronic mail addresses; social security numbers; medical record numbers; web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; and so on. In addition, the relevant entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual.[174]

ALRC's view

58.166 The ALRC has considered the definitions of 're-identifiable data' and 'non-identifiable data' in the National Statement and has formed the view that it is unnecessary to include definitions of these terms in the *Privacy Act.* The issue of whether information is identified, reasonably identifiable, re-identifiable or non-identifiable is contextual and so must be considered on a case-by-case basis. This includes making a distinction between information that may be re-identifiable in a particular context—for example, where an agency or organisation holds information identified by a unique identifier and also holds the master list—but is not reasonably identifiable for the purposes of the Act in another context—for example, where an agency or organisation holds information identified by a unique identifier but does not hold and does not have access to the master list.

58.167 The ALRC notes that this last category of information falls into the National Statement's 'non-identifiable' category. For the purposes of the *Privacy Act*, however, it is sufficient to regard the information as 'not reasonably identifiable'. If the risk of identification from particular information in a particular context is very small, a decision will have to be taken as to whether, on objective grounds, the information is 'reasonably identifiable'. Agencies and organisations will be required to make such decisions and will need to ensure that they have the appropriate knowledge and experience to be able to do this.

---

173 *Health Insurance Portability and Accountability Act of 1996* Pub L 104–191, 110 Stat 1936 (US) s 164.514(b)(1).

174 Ibid s 164.514(b)(2).

58.168 The ALRC's view is that guidance provided by the Privacy Commissioner would be of great value to those making decisions on a case-by-case basis on these matters. Such guidance might refer to or include guidance of the sort provided in the National Statistical Service Handbook[175] or the provisions of the HIPA Act discussed above. The ALRC is of the view that providing guidance rather than legislative rules allows a more flexible and nuanced response to particular situations.

58.169 In ALRC 96, the ALRC and AHEC considered the use of independent intermediaries to hold codes linking genetic samples or information with identifiers. ALRC 96 concluded that use of an independent intermediary (such as a 'gene trustee') is an effective method of protecting the privacy of samples and information held in human genetic research databases. The system maintains the privacy of samples and information, while allowing donors to be contacted if necessary. It ensures that anyone who obtains access to samples and information is unable to re-identify them without the authorisation of the gene trustee.[176]

58.170 The ALRC's view is that this kind of arrangement might also provide appropriate protection in relation to other personal information, but this will depend on the arrangements established between data custodians, intermediaries and data recipients. If appropriate arrangements are put in place, such that data recipients are not able to identify individuals, the ALRC is of the view that the information held by the data recipient is likely to be not reasonably identifiable in that context and no longer 'personal information' for the purposes of the *Privacy Act.*

Proposal 58–10 The Privacy Commissioner should provide guidance on the meaning of 'not reasonably identifiable'.

Databases and data linkage

Establishing databases

58.171 Health databases and registers may be established for a number of reasons in both the health services and the health and medical research contexts. The National Health Information Management Group has defined a 'health register' as follows:

> For the purposes of these guidelines, a health register is a collection of records containing data about aspects of the health of individual persons. The subjects will typically be patients or clients of a health service or health program, from which the data are collected. Health registers are characterised by being:

175 National Statistical Service, *National Statistical Service Handbook* <www.nss.gov.au/nss/home.NSF/pages/NSS+Resources?OpenDocument> at 1 August 2007.

176 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [18.102]–[18.117].

> *personal data* each record represents a person, not a set of aggregated data;
>
> *identified* each record in the register is identified to a particular subject;
>
> *population-based* the register aims to include a record of all persons within its defined scope; populations may be broadly or narrowly defined, e.g. Australia wide, regionally based or clients of a local service; and
>
> *ongoing* collection is not restricted to a particular period of time.[177]

58.172 Dr Roger Magnusson defines health registers as 'discrete repositories of information separate from clinical records' but notes that the distinction between clinical records and data registers is likely to diminish as health records gradually become databases.[178] The establishment and management of electronic health information systems and shared electronic health records in the health services context are discussed in Chapter 56.

58.173 A number of health information databases and registers have been established by legislation. As noted above, the Australian Government maintains the Medicare and Pharmaceutical Benefits Program databases. State and territory governments in Australia have established databases that include information collected under mandatory reporting requirements in public health legislation. For example, the *Public Health Act 1991* (NSW) requires health service providers to notify the cervical cancer register of cervical cancer screening tests performed and the results of those tests. The Act states that the purpose of the register is to reduce the incidence of, and mortality from, preventable cervical cancer.[179]

58.174 A wide range of non-statutory databases collect information on a voluntary basis and may be established and maintained by hospitals, universities, research bodies and others. For example, the Australian and New Zealand Dialysis and Transplant Registry (ANZDATA) records the incidence, prevalence and outcome of dialysis and transplant treatment for patients with end stage renal failure.[180] The Menzies Centre for Population Research maintains a research database comprising extensive genealogical data, genetic samples, and health information supplied by donors, to search for genetic causes of disease. All material is provided with consent specifically for the Centre's research projects.

58.175 Health service providers, such as hospitals, also maintain extensive databases established in the course of delivering health services and for management, funding and monitoring purposes.

---

177 Australian Institute of Health and Welfare, *Minimum Guidelines for Health Registers for Statistical and Research Purposes* (2001), 2.

178 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 15.

179 *Public Health Act 1991* (NSW) s 42G.

180 ANZDATA is located at The Queen Elizabeth Hospital in South Australia.

58.176 In its submission to the OPC Review, the NHMRC noted that access to health information in such registers is crucial to the conduct of public health research but expressed concern that the *Privacy Act* does not provide an appropriate regime for the establishment, maintenance and use of such registers.

58.177 The NHMRC stated that the use or disclosure of health information without consent for the purposes of establishing or maintaining a register is unlikely to comply with the NPPs. Such use and disclosure is unlikely to be a directly related secondary purpose or to be within the reasonable expectations of health consumers. The NHMRC noted that getting consent from all relevant health consumers for their health information to be included in a register is likely to be impracticable and that incomplete data sets substantially impair the utility of such registers.[181]

58.178 The NHMRC noted that such registers would appear to require approval by an HREC, according to the Section 95A Guidelines, but that it would be difficult for an HREC to decide where the balance of interests lay in relation to an individual register, in the absence of specific information about the proposed future use of the register. The NHMRC noted that health information registers raise significant privacy concerns, but considered that the registers should be permitted within a rigorous ethical and privacy framework that appropriately protects the public interest.[182]

58.179 In ALRC 96, the ALRC and AHEC gave detailed consideration to the regulation of human genetic research databases, including the issue of consent to future unspecified use of information held in such databases. ALRC 96 made a number of recommendations in this regard, including:

> The National Health and Medical Research Council (NHMRC), as part of its review of the *National Statement on Ethical Conduct in Research Involving Humans* (the National Statement) in the 2003–2005 triennium, should amend the National Statement to provide ethical guidance on the establishment, governance and operation of human genetic research databases. The amendments (whether by means of a new chapter or otherwise) should include specific guidance on obtaining consent to unspecified future research.[183]

58.180 The 2007 National Statement does include a chapter on 'databanks'.[184] The chapter discusses establishing databanks and using the information stored in databanks

---

181 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

182 Ibid. The Australian Nursing Federation was also of the view that collection of data for health data registers is being impeded by individual organisations' interpretation of the *Privacy Act*. Australian Nursing Federation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 1 February 2005.

183 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 18–1.

184 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), Ch 3.2.

for research purposes. The National Statement discusses consent requirements for collection of information into databanks, including: 'specific consent' that is limited to a specific research project; 'extended consent' for the use of information in future research projects that are closely related to the original project or in the same general area of research; and 'unspecified consent' for the use of information for any future research. The National Statement includes specific guidance on obtaining such consent and notes the possibility that a researcher may seek permission from an ethical review body to proceed without consent.[185]

Submissions and consultations

58.181 In its submission, the OPC acknowledged that seeking approval to establish a health register through the HREC mechanism may present difficulties:

> In the absence of a clearly identified purpose, HRECs would be unable to assess where the public interest lay in relation to the register. It may be difficult for researchers to clearly identify all prospective uses of that data at the time of submitting a research proposal. As the NHMRC put it in their submission to the OPC review, 'by the time the questions are obvious, the opportunity to identify the person to whom the information relates or to gain consent to use the health information may be lost'.[186]

58.182 The OPC expressed the view that specific legislative provision should be made for the establishment of health data registers and that enabling legislation would bring the activity within the 'required or authorised by law' exception in NPP 10. The OPC stated that establishing such registers under specific legislation would offer 'the certainty, parliamentary oversight and scrutiny needed to sustain community confidence'.[187]

58.183 In addition to reiterating its concern that the *Privacy Act* does not provide an appropriate and effective regime for the establishment and use of health data registers, the NHMRC also stated in its submission to this Inquiry that:

> We consider that there is an urgent need for the development of a binding National Standard for the Establishment and Management of Health Information Registers and Data Linkage, addressing, amongst other issues, the collection, use (including linking) and disclosure of health information for research purposes, in the absence of consent.[188]

58.184 The AIHW agreed with the NHMRC that the existing provisions of the *Privacy Act* do not provide an appropriate regime for the establishment, maintenance and use of health registers. The AIHW was also of the view that such registers should

---

185 Ibid, [2.2.14].

186 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

187 Ibid.

188 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007. The Queensland Institute of Medical Research, *Submission PR 80,* 11 January 2006 expressed support for this approach.

be able to be developed and used without consent within a strict privacy and ethical framework.[189]

58.185 The Western Australian Department of Health expressed the view that:

> Guidelines are needed to assist HRECs with the application of the public interest test to research infrastructure projects such as long term data bases or biobanks. In these cases the benefits of the research cannot be effectively evaluated because particular research projects are prospective and have not yet been developed. The value of the research is therefore speculative. Factors relevant to evaluating the public interest in these applications should include the administrative procedures for managing and securing the data over the life of the data bank or biobank, the provision of information to participants, the criteria for access and the procedures for protecting privacy.[190]

58.186 DOHA was of the view that, where collection of personal information into a research database was to be mandatory and done without consent, the database should be established by specific legislative provisions.[191]

ALRC's view

58.187 In Chapter 57, the ALRC proposes that the *Privacy (Health Information) Regulations* make express provision for the collection, use and disclosure of health information without consent where necessary for the funding, management, planning, monitoring, improvement or evaluation of a health service where:

- the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual;
- it is impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and
- the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner for the purposes of the regulations.[192]

58.188 This provision would allow the establishment of health information databases and registers in the health services context where it is necessary to collect identified information and it is not practicable to seek consent. Establishing a database under this proposed provision would not require approval by an HREC, although it would have to be done in accordance with rules issued by the Privacy Commissioner.

---

189 Australian Institute of Health and Welfare, *Submission PR 170,* 5 February 2007.
190 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.
191 Australian Government Department of Health and Ageing, *Submission PR 273,* 30 March 2007.
192 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Proposal 57–9.

58.189 The ALRC notes that it will continue to be possible to establish particular databases or registers in the health services context or the research context by legislation, as has been done in the case of the New South Wales cervical cancer register. It will also continue to be possible to establish databases or registers on the basis of consent, including specific, extended or unspecified consent as set out in the National Statement.

58.190 Where such a database is to be established for research purposes and the information is to be collected, used or disclosed without consent, this will also be possible under the proposed research exceptions to the UPPs, but will require the approval of an HREC and will have to be done in accordance with rules issued by the Privacy Commissioner.

58.191 The ALRC notes the NHMRC's concern that it is sometimes difficult for an HREC to decide where the balance of interests lies in relation to an individual register, in the absence of specific information about the proposed future use of the register. Proposals 58–8 and 58–9, above, provide that HRECs consider the public interest in a proposed collection, use or disclosure of health information without consent where it is 'necessary to research', and be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs. The language used in the proposals is deliberately broad, referring to the review of 'activities necessary for research', rather than review of specific research proposals in order to allow the review of activities preliminary to research, such as the establishment of registers or sample acquisition, discussed below.

58.192 In addition, Proposal 58–3 suggests that the definition of research should include the 'compilation and analysis of statistics'. The establishment of a database or register for research purposes might also be characterised as the 'compilation of statistics' and reviewed on that basis.

58.193 The ALRC is of the view, however, that such databases or registers should not be established in the research context in the absence of legislation or ethical review. Both these mechanisms provide a degree of scrutiny and balancing of public interests that is appropriate where personal information, including sensitive information such as health information, is to be collected, used and disclosed without consent by researchers. The ALRC's view is that researchers proposing to establish databases or registers for research purposes should be able to describe the potential future uses and benefits of the database at some level and to provide an HREC with enough information to allow the HREC to consider whether the public interest in establishing the database outweighs the public interest in maintaining the level of privacy protection provided by the UPPs. If the public interest in establishing the database cannot be demonstrated, the ALRC is of the view that the UPPs should prevail. In these circumstances it may be more appropriate to proceed on the basis of consent.

58.194 The ALRC notes that it would also be possible to seek a PID from the Privacy Commissioner to allow the establishment for research of databases or registers, or a particular database or register. This process would also provide scrutiny and the opportunity to weigh the competing public interests.

58.195 The ALRC's view is that the rules to be issued by the Privacy Commissioner under the research exception to the UPPs should address the process by which an HREC might review a proposal to establish a database or register for research purposes, as well as the matters an HREC should take into account in considering the public interest balance. The ALRC is of the view that the rules should make clear that where a database or register is established without consent on the basis of HREC approval, that approval does not extend to future unspecified uses. Any future uses of the database or register for research would require separate consideration.

58.196 The rules to be issued by the Privacy Commissioner in relation to the collection of sensitive information without consent for research might include standards for the establishment and management of health information registers as suggested by the NHMRC. It would be open to the Privacy Commissioner to develop such standards in consultation with stakeholders.

Proposal 58–11 The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:

(a) the process by which a Human Research Ethics Committee should review a proposal to establish a health information database or register for research purposes;

(b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in establishing the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

(c) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

Using and linking information in databases

58.197 Databases of health information provide the opportunity to link data more effectively. Dr Roger Magnusson notes that:

> Future improvements in public health will increasingly depend on the more effective use of health data resources: in order to monitor trends in health status, to investigate the causal roles of 'lifestyle', environmental and other risk factors … to measure and improve the quality and performance of health care services and to develop 'best practice' for prevention and care. Epidemiologists and population health researchers, in particular, are keen to unlock the public health value of clinical data …[193]
>
> Identifying and investigating the relationships between risk factors and disease frequently requires researchers to accurately match longitudinal data relating to the same individual.[194]

58.198 The National Health Information Management Group Guidelines note that:

> Most [health registers] will be intended to facilitate further research, for example, through record linkage to other data sets or establishing a sample frame for a more detailed study of a health problem or for clinical trials.[195]

58.199 The National Collaborative Research Infrastructure Strategy (NCRIS) is an Australian Government program announced in 2004 with funding of $542 million to 'provide researchers with major research facilities, supporting infrastructure and networks necessary for world-class research'.[196] One major focus of the Strategy is population health and clinical data linkage:

> Australia is an international leader in the scope and extent of health-related data collected at the population level. With new technologies, the potential exists to integrate and link data sets, providing a valuable new resource for monitoring the health of the population and the effectiveness of health services, and for research.
>
> The NCRIS *Population health and clinical data linkage* capability aims: to enhance the linkage and integration of health-related data collected in Australia; to provide improved accessibility to these data for the research sector; and to support the development of improved data collection systems.[197]

58.200 The *Privacy Act*, like the National Statement, recognises that in some circumstances it is very difficult or impossible to conduct this kind of research in a way that complies with the IPPs and NPPs. As discussed above, the *Privacy Act* provides a mechanism to allow such research to go forward on the basis of approval by an HREC. The National Statement also requires that, where information in a databank is stored in identified or identifiable form, any research proposing to make use of the information be ethically reviewed.

58.201 In its submission to the OPC Review, the NHMRC noted that some HRECs appear to reject research proposals automatically where they involve data linkage of

---

193 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 8.

194 Ibid, 11.

195 Australian Institute of Health and Welfare, *Minimum Guidelines for Health Registers for Statistical and Research Purposes* (2001), 2.

196 Australian Government Department of Education Science and Training, *National Collaborative Research Infrastructure Strategy* <www.ncris.dest.gov.au/> at 1 August 2007.

197 Ibid.

health information without consent, apparently in the 'mistaken belief that such linkage is not ethically or legally acceptable'.[198] The revised National Statement makes clear that approval may be given to use such data even in the absence of consent, for example, where the research involves linkage of data sets and the use of identifiable data is necessary to ensure that the linkage is accurate.[199]

58.202 The NHMRC also highlighted a particular problem for researchers in gaining access to data registers in order to identify health consumers with specific characteristics relevant to a research proposal. This activity, described as 'sample acquisition', may pre-date the development of a formal research proposal and, in the NHMRC's view, is unlikely to be consistent with the IPPs or NPPs. The NHMRC considers, however, that sample acquisition is important and should be facilitated by the *Privacy Act*.[200]

Submissions and consultations

58.203 One stakeholder noted that the process of linking health information for research could be distinguished from the linking of health information for clinical purposes. Those delivering clinical care need to know the identity of the individual and to have access to that individual's health information. Researchers generally do not need to know the identity of the individual, simply that certain health information relates to the same individual. This can be achieved through processes whereby those who perform the linking of information do not have access to the health information and researchers have access to the linked health information but not the identity of the individual.[201]

58.204 In ALRC 96, the ALRC and AHEC considered the use of independent intermediaries to hold codes linking genetic samples or information with identifiers. ALRC 96 concluded that use of an independent intermediary (such as a 'gene trustee') is an effective method of protecting the privacy of samples and information held in human genetic research databases. The system maintains the privacy of samples and information, while allowing donors to be contacted if necessary. It ensures that anyone who obtains access to samples and information is unable to re-identify them without the authorisation of the gene trustee.[202] ALRC 96 recommended that:

> The NHMRC, in revising the National Statement in accordance with Recommendation 18–1, should provide guidance on the circumstances in which the

198 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

199 National Health and Medical Research Council, Australian Research Council and Australian Vice Chancellors' Committee, *National Statement on Ethical Conduct in Human Research* (2007), [3.2.4].

200 National Health and Medical Research Council, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 10 December 2004.

201 A Smith, *Submission PR 79,* 2 January 2007.

202 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [18.102]–[18.117].

> use of an independent intermediary is to be a condition of: (a) registration of a human genetic research database; or (b) approval by an Human Research Ethics Committee of research involving a human genetic research database.[203]

58.205 In its submission to this Inquiry, the NHMRC expressed support for these conclusions and noted that they also applied more broadly to non-genetic research databases.[204]

58.206 In its submission, the CSIRO noted the development of the DLU in Western Australia and the New South Wales/ACT Centre for Health Record Linkage and noted that such units are likely to increase through the NCRIS Population Health and Clinical Data Linkage program.[205]

58.207 The DLU is a co-operative scheme between the Information Collection and Management Branch at the Western Australian Department of Health, the Centre for Health Services Research at the University of Western Australia, the Division of Health Sciences at Curtin University of Technology, and the Telethon Institute for Child Health Research. The DLU was established in 1995 to develop and maintain a system of linkages connecting health information about individuals in Western Australia. The DLU's website states that:

> These linkages are created and maintained using rigorous internationally accepted privacy-sensitive protocols, probabilistic matching and extensive clerical review. The core Data Linkage System consists of links within and between the State's seven core population health datasets, spanning 35 years. This is augmented through links to an extensive collection of external research and clinical datasets. Data can be requested for ethically approved research, planning and evaluation projects, which aim to improve the health of Western Australians.[206]

58.208 In its submission, the Western Australian Department of Health noted that the:

> DLU uses a two stage data linkage protocol that allows linkage infrastructure (or linkage keys) to be created using identifying information. Linkable datasets containing encrypted identifiers can then be provided to researchers by data custodians with minimal risk of re-identification or unauthorized linkage to another data source. The linkage infrastructure is updated and managed separately from any clinical or service information. The DLU acts as an intermediary similar to a 'gene trustee'. Ethics clearance is required for the creation of new linkages and use of the linkage infrastructure.[207]

58.209 The DLU has now entered into an arrangement with the Australian Government to allow access to Australian Government held aged care information as

---

203 Ibid, Rec 18–3.
204 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.
205 CSIRO, *Submission PR 176,* 6 February 2007.
206 University of Western Australia—School of Population Health, *WA Data Linkage Unit* <www.populationhealth.uwa.edu.au/welcome/research/dlu/linkage> at 1 August 2007.
207 Department of Health Western Australia, *Submission PR 139,* 23 January 2006.

well as information in the Medicare Benefits Scheme and the Pharmaceutical Benefits Scheme databases. The Western Australian Department of Health and DOHA have entered into a Memorandum of Understanding (MOU) formalising the arrangements and a 'best practice protocol' has been developed to address privacy concerns and other issues.[208]

58.210 In its submission,[209] however, the OPC expressed the view that the method employed by the DLU would not be consistent with NPP 10.4, which provides:

> If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

58.211 The OPC's view is based on the requirement that the information is 'permanently de-identified'. The maintenance of the linkage infrastructure means that information is not permanently de-identified even though a researcher takes reasonable steps to ensure that the information is not disclosed in a form that would identify individuals or from which individuals could be reasonably identifiable. The linkage infrastructure can technically be used to re-identify the information, although this could only be done with the cooperation of the DLU. In ALRC 96, the ALRC and AHEC concluded that maintaining the linkage infrastructure can be important in order to allow individuals to be contacted if research produces information that is of importance to the future health of those individuals.[210]

58.212 The Centre for Health Record Linkage is a co-operative scheme established by NSW Health, the Cancer Institute NSW, the Clinical Excellence Commission, the University of Sydney, the University of New South Wales, the University of Newcastle, ACT Health and The Sax Institute. The Centre, like the DLU, will create master linkage keys allowing researchers to link information about particular individuals in different databases in New South Wales and the ACT without being able to identify the individuals.

58.213 In its submission, the CSIRO discussed another data linkage model that offered researchers access to information within a privacy protective environment:

> In recognition of the widespread challenge of generating information from databases which include personal information and at the same time not compromising standards of privacy and confidentiality, CSIRO has been developing new privacy-enhancing technologies, including:

---

208 University of Western Australia—School of Population Health, *WA Data Linkage Unit* <www.populationhealth.uwa.edu.au/welcome/research/dlu/linkage> at 1 August 2007.

209 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

210 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 16.

- Health Data Integration™ (HDI™)—software which enables linking of patient records from different data repositories without requiring identifying information to be revealed to any other party. Any external release of the data through HDI™ is controlled by the data custodian, and can be stopped at any time.
- Privacy-Preserving Analytics™ (PPA™)—software developed for analysing confidential data without compromising confidentiality. The PPA techniques allow analysis of confidential raw data, but filter the outputs delivered to the researcher in order to protect the privacy of individuals and organisations and to respect data custodians' responsibilities not to release confidential information.[211]

58.214 There are also other models being used around Australia such as the Bio21: Molecular Medicine Informatics Model (MMIM) currently being piloted in Victoria, that aims to allow authorised researchers to conduct research 'confident that ethics, privacy, security and IP issues are addressed'. The Bio21: MMIM website states that the model will provide

> clinical research collaborators from universities, research institutes and teaching hospitals with ethical approval [with] access [to] secure, privacy protected research information, that spans multiple disease groups and multiple organisations.[212]

58.215 The Department of Human Services suggested that:

> There is little guidance in the *Privacy Act* for these issues, which leads to differing interpretations being made by organisations dealing with health registers. A set of minimum standards should be developed to facilitate effective/safe linkage processes to allow important research to be conducted, without identifying particular individuals where no consent has been obtained. Medicare Australia believes the example presented by the Cross-Jurisdictional Linkage of Administrative Health Data project, underpinned by an MoU between DoHA and WA Department of Health, could be a good model on which to base the set of minimum standards.[213]

58.216 In relation to sample acquisition, that is, the examination of health information databases to identify health consumers with characteristics relevant to a possible research proposal, the OPC noted that the research exceptions in NPPs 2 and 10 cover activities *necessary* for research, and expressed the view that sample acquisition was such an activity and would be covered by the exceptions. The OPC noted, however, that sample acquisition might not be covered by the 'conduct of medical research' exception to the IPPs.[214]

ALRC's view

58.217 The ALRC agrees that 'sample acquisition' is an activity necessary for research and should be supported by the provisions of the *Privacy Act.* The ALRC

---

211 CSIRO, *Submission PR 176,* 6 February 2007.

212 Melbourne Health, *Molecular Medicine Informatics Model* (2007) <mmim.ssg.org.au/> at 1 August 2007.

213 Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

214 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

notes the OPC's advice that this activity is allowed under the existing provisions of NPPs 2 and 10. The ALRC's view is that the proposed research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle set out in Proposals 58–8 and 58–9 clarify the position, as the proposed exceptions apply to 'activities necessary for research'.

58.218 The ALRC is of the view that the rules to be issued by the Privacy Commissioner under the research exceptions to the UPPs could address the process by which an HREC might review a sample acquisition proposal, as well as the matters an HREC should take into account in considering the public interest balance.

58.219 Proposal 58–8, above, also includes a suggested amendment to the wording of NPP 10.4, so that the provision no longer requires that reasonable steps be taken 'to permanently de-identify' information before it is disclosed. The ALRC's view is that it is sufficient to require agencies and organisations that collect sensitive information under the research exception to the proposed 'Collection' principle to take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

58.220 An amendment of this kind would allow researchers to access information through independent intermediaries without requiring the destruction of the linkage infrastructure. As noted above, however, it will be necessary to consider the arrangements established between data custodians, intermediaries and data recipients. If appropriate arrangements are put in place, for example, intermediaries are sufficiently independent and data recipients only receive information that does not identify individuals, the ALRC's view is that the information held by the data recipient will be adequately protected for the purposes of the *Privacy Act*.

58.221 There are a number of different models being adopted around Australia to allow researchers to have access to and to link personal information in ways that do not identify individuals. The ALRC has not formed a view that one model should be preferred over another. It is possible that each of the various models provide sufficient protection to ensure that the schemes they support comply with the *Privacy Act*. That will depend, however, on the details of the various models, their technical specifications and their governance arrangements.

58.222 Some high level guidance on these issues may be included in the rules to be issued by the Privacy Commissioner under the proposed research exceptions to the UPPs, but in the final analysis whether a particular model meets the requirements of the *Privacy Act* will have to be decided on a case-by-case basis. These issues will need to be considered by HRECs in reviewing proposals to collect, use or disclose personal information without consent.

58.223 The ALRC is also of the view that agencies or organisations seeking to establish systems or infrastructure to allow the linkage of personal information for research purposes, should consult the OPC to ensure that the systems or infrastructure they are developing meet the requirements of the *Privacy Act*.

Proposal 58–12 The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:

(a) the process by which a Human Research Ethics Committee should review a proposal to examine a health information database or register to identify potential participants in research; and

(b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in allowing the examination of the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.

Proposal 58–13 Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should consult the Office of the Privacy Commissioner to ensure that the systems or infrastructure they are developing meet the requirements of the *Privacy Act*.

59. Children, Young People and Privacy

Contents

Introduction 1715
Generational difference 1716
Attitudes of young people 1719
Australian research 1719
Overseas research 1720
ALRC consultations with young people 1723
Talking Privacy website 1723
Youth workshops 1724
Submissions and other consultations 1726
Online social networking 1728
Privacy concerns about online social networking 1728
Choosing to disclose 1730
Regulatory options 1732
The need for education 1734
Photographs and other images 1735
Background 1735
Submissions and consultations 1737
Options for reform 1738
ALRC's view 1744
An ongoing study of attitudes to privacy 1744
Online social networking 1746
Photographs and other images 1746
Privacy education for children and young people 1748

Introduction

59.1 During the early stages of this Inquiry, the ALRC was told anecdotally that young people think of privacy differently from older generations. If this is true, there may be consequences for the development of proposals for privacy that meet the current and future needs of Australians. It was therefore important that the Inquiry make some effort to capture the attitudes to privacy of Australian children and young people, highlight the issues about which they have concerns, and consider the implications for the broader reform of privacy law.

59.2 This chapter will set out the methods the ALRC used to consult with children and young people, and the findings of those consultations and other research. This

information has led to a number of proposals, the first of which is the need for a longitudinal study of the privacy attitudes of Australians, including young people, to underpin future policy making in this area.

59.3 One of the areas of concern that arose during consultations and in research was the participation of young people in online social networking. The ALRC has identified this as an area where improved education and awareness of privacy issues will assist young people to make appropriate choices in the online environment. The ALRC has made a number of proposals aimed at achieving this outcome.

59.4 Another area of concern is the taking of photographs and other images and, in particular, the online publication of photographs and other images. This issue raises problems of a criminal nature as well as concerns regarding invasion of privacy. With a focus on the privacy aspects of the issue, this chapter canvasses a number of reform options, but does not make any specific proposals relating to the taking and publishing of photographs and other images. Instead, the chapter links to discussion and proposals in other chapters which the ALRC considers will provide the most effective remedies. Such proposals include a statutory cause of action for invasion of privacy, and the consideration of using take-down notices to remove online content that is considered to be an invasion of privacy.

59.5 In this chapter, the term 'child' refers to a person under the age of 13. The term 'young person' encompasses people aged 13 to 25. Chapter 60 deals specifically with issues about individuals under the age of 18 making decisions in relation to the *Privacy Act 1988* (Cth).

Generational difference

59.6 In the past few years the phenomenon of Generation Y, the label given to the generation of people born between 1980 and 1994, has generated a great deal of discussion. As they enter adulthood and the workforce, social researchers are trying to understand the psyche of this group of young people. While not privacy specific, this research can help to develop an understanding of how this group might perceive privacy issues in the wider context of their experiences, needs, and ambitions.

59.7 Generational definitions are, by necessity, broad brush generalisations. There always will be individuals who do not fit the stereotype merely because of they were born in a particular year. Generational definitions, however, may be useful to gain a sense of the key social drivers and expectations across certain sections of the population.

Table 59.1: Australia's Generations[1]

Description	Born	Age	Pop'n	(% of Pop'n)
Builders	Before 1946	62+	3.5m	17%
Boomers	1946–1964	43–61	5.3m	26%
Generation X	1965–1979	28–42	4.4m	21.5%
Generation Y	1980–1994	13–27	4.2m	20.5%
Generation Z	1995–2009	Under 13	3.1m	15%

59.8 Generations traditionally have been defined by intervals of time between the birth of a parent and birth of the offspring. Social researchers today, however, focus on cohorts of people born and shaped by a particular span of time, with demographical and sociological definitions. When carrying out social research in Australia, McCrindle Research has used Australian Bureau of Statistics data to map birth rate rises and declines to mark distinct generational definitions. Social changes and trends affecting these cohorts provide context for the generational definition.

59.9 Some of the key characteristics often attributed to Generation Y are as follows:[2]

- While older generations have adapted to new technology, Generation Y lives and breathes the internet, email, instant messaging and mobile technologies that have revolutionised communications. Generation Y have never known a world without these conveniences, and their social world and expectations are integrated with the existence of such technology.

- Having experienced (either themselves or through their friends) split households and working parents, social networks of friends have become the most important element of the lives of Generation Y, and they keep in touch constantly using technology.

- Generation Y lives in a global village, where you can communicate across the globe through a variety of instantaneous media, and is considered the most embracing, non-racist, non-gender biased generation yet.

---

1 Table 59–1 is based on a similar table in McCrindle Research, *New Generations at Work: Attracting, Recruiting & Training Generation Y* (2006), 8. In the United States, the Builders are often referred to as the 'Silent Generation'.

2 See, eg, Ibid; R Huntley, *The World According to Y: Inside the New Adult Generation* (2006); N Howe and W Strauss, *Millennials Rising: The Next Great Generation* (2000).

- Generation Y have very high levels of optimism, high expectations and confidence they will achieve those expectations. This can be compared to Generation X which is viewed as being apathetic and pessimistic.

- On the back of high self confidence, Generation Y is considered fickle and demanding, and willing to move quickly to take up new opportunities.

59.10 A common counter to generational research is that many of the attributes applied to young people at any given time are really factors associated with youth itself, not the particular generation. For example, the dependence on friends as social networks is a normal part of the teenage years, but it is said that Generation Y are taking it with them into the adult years and honestly believe that those friends will remain friends for life. Generation X was labelled by their elders as apathetic and pessimistic, or 'slackers', and such behaviour was seen as a normal part of teenage development. It is said that the difference between Generation X and Baby Boomer attitudes has persisted as Generation X has come to full adulthood. In contrast, teenage Generation Y is considered a 'selfless' generation, with a strong community service ethic.[3]

59.11 Australian social researcher Hugh Mackay has contrasted the attitudes of 19 year olds in 1980 and 2000, finding a distinct attitude shift from pessimism to optimism.[4] The 1980 cohort were pre-occupied with the state of the world, the threat of nuclear annihilation, widespread terrorist activity, growing economic dislocation and recurring industrial trouble, while the 2000 cohort were utterly confident about their own, and the world's, long-term survival. Even after the events of 11 September 2001, the 2002 Bali bombings and the 2006 London bombings, Dr Rebecca Huntley suggests that today's young adults have a sense of optimism and confidence and are either more capable of facing the world's problems or more effective at ignoring them.[5]

> In Australia, Generation Y's anger around [September] 11 was less about the event itself than the reaction of the United States government and its allies. Many young adults have reacted negatively to the media hype around the tragedy and the relentless and insensitive use of images of death and destruction to sell papers and increase TV ratings. And whilst this was Generation Y's first exposure to international terrorism on a grand scale, most Yers were aware that in so many other places around the world this kind of stuff happens all the time. For many of them now, September 11 intensified their desire to enjoy life right now.[6]

59.12 While commentators can make generalisations about the attitudes of Generation Y, it remains unknown whether those attitudes are wide-spread and will remain with these young people as they enter their late 20s, 30s and 40s and experience different stages of their lives. What can be said is that their experiences will be

---

3 N Howe and W Strauss, *Millennials Rising: The Next Great Generation* (2000), 214–219.
4 H Mackay, *The Mackay Report: Leaving School* (2000), 26.
5 R Huntley, *The World According to Y: Inside the New Adult Generation* (2006), 9.
6 Ibid, 4.

different from those of generations before because they have started from a different place in space and time.

Attitudes of young people

Australian research

59.13 The ALRC is not aware of any available Australian research which focuses on the attitudes of young people to privacy.[7] However, a number of general surveys on attitudes to privacy provide some indication of how the 18–24 age group perceive privacy.

59.14 The Office of the Privacy Commissioner (OPC) has conducted three surveys of community attitudes on privacy, but all of these involved only adult respondents.[8] The 2001 and 2004 surveys, however, did separate data by age groups. The following sets out some of the key points from the 2004 survey:

- Young people were as likely as the rest of the adult population to claim they know very little about their rights to protect their personal information—but the percentage of this age group making the claim dropped significantly from 52% in 2001 to 36% in 2004.[9]

- Young people were less likely than other age groups to claim to be aware of federal privacy laws and the federal Privacy Commissioner.[10]

- Young people were less concerned about providing financial details than older respondents (30% of 18–24 group compared with 42% of 35–49 group and 45% of 50+ group), but much more concerned about providing contact details such as home address (18% of 18–24 group compared with 6% of 35–49 group and 4% of 50+ group) or email address (7% of 18–24 group compared with 5% of 35–49 group and 3% of 50+ group).[11]

- Young people were much more likely to provide personal information to an organisation in order to receive a discount or a more efficient and personalised service. The percentages dropped steadily through the age groups. For example,

---

7 An online survey aimed at young people was commenced in June 2007 by the United Nations Youth Association in South Australia, the Flinders Law Students Association, and the Adelaide Law Students Society. Outcomes of the survey will be provided to the ALRC when available.

8 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004); Roy Morgan Research, *Privacy and the Community [prepared for Office of the Federal Privacy Commissioner]* (2001). A similar survey was conducted by Roy Morgan in 1999.

9 Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 11.

10 Ibid, 12–13.

11 Ibid, 25.

to obtain a personalised service 66% of the 18–24 group indicated they would provide the personal information, while only 32% of the 50+ group agreed.[12]

- While young people were as likely as other age groups to agree to allocation of a health number to track health services, they were more likely than older age groups to feel inclusion of health records on a database should be voluntary.[13]

- Young people were much more likely to have engaged in online behaviour that can protect privacy, such as providing false information when filling out a form online, using a spam filter or using temporary email accounts.[14]

59.15 A 2005 survey of the use of the internet and some other forms of technology by Australian children and young people, particularly those aged 8 to 13, is also of interest.[15] The survey found that, while Australian children are not accessing the internet as frequently as children in Hong Kong or the United Kingdom, the frequency of use has increased. Thirty seven per cent of children with a home internet connection reportedly log on daily, and a further 34% log on at least two or three times a week. The survey also showed that frequency of use increased with age; and that girls and older children were more likely to use the internet as a communication resource (for email and instant messaging) than boys and younger children—who were more focused on access for entertainment purposes (games, websites, music).

59.16 While not focused on privacy, the survey does indicate that large numbers of Australian children and young people are making regular use of online technology, in some cases with limited or no supervision. A more recent 2006 survey by the Australian Bureau of Statistics echoes the significant use of the internet by children aged 5 to 14 years. Sixty five per cent of this age group access the internet, with 73% of the online group accessing it more than once a week.[16]

Overseas research

59.17 One example of overseas research focusing on attitudes of young people to privacy is a 2005 survey by the Hong Kong Federation of Youth Groups and the Hong Kong Office of the Privacy Commissioner for Personal Data which included respondents aged 15 to 29.[17] There is no comparative survey for older people. While it was a limited survey, with a particular emphasis on online transactions, the results indicate that young people in Hong Kong appear to have similar attitudes to privacy as

12 Ibid, 36–37.
13 Ibid, 48–49.
14 Ibid, 64–66.
15 Netratings Australia Pty Ltd, *kidsonline@home: Internet Use in Australian Homes [prepared for Australian Broadcasting Authority and NetAlert Limited]* (2005).
16 Australian Bureau of Statistics, *Children's Participation in Cultural and Leisure Activities, Australia, Apr 2006*, 4901.0 (2006).
17 Hong Kong Federation of Youth Groups, *2005 Survey of Youth Attitudes and Perceptions Towards Personal Data Privacy* (2005).

young people in Australia—that is, they have an awareness of privacy law, have concerns about certain privacy issues, but many also consider certain types of initiatives, such as a patient medical records database, to be worth participating in. Of particular interest in the survey were two questions regarding the taking of photographs by strangers. 14.4% of respondents admitted to having taken a photo of a stranger without first asking permission, and 21.3% disagreed or strongly disagreed with the suggestion that taking a photo of a person in a public place without permission is an invasion of personal data privacy rights.[18] There was no age breakdown of responses to these questions to see if responses differed according to age.

59.18 Privacy issues for young people have also been addressed in the United States as part of a broader study of 'the lives of young Americans as they make the transition to adulthood'.[19] Surveying 1,021 adults aged 18–24 years in April 2006, the researchers reported that the respondents generally valued privacy, but evenly weighed it with the ease and convenience the internet provides.[20] Seventy-eight percent indicated that they had a personal website, webpage or blog and regularly participated in online communities such as MySpace or Facebook. Those who did not belong to online communities were more likely to place a higher value on privacy over convenience.

59.19 The research suggested that Generation Y balances privacy and convenience concerns by taking personal responsibility for safe behaviour and self-censoring the type of personal information made available online. At the same time, many from older generations would blanche at the level of detail and the types of information young people feel comfortable about sharing, including 16% posting their home address online and 78% posting photos (often unflattering or 'sexy' photos). The concerns of young people in the online environment appeared to be more closely linked to identity theft and receiving spam than stalking and harassment (although the latter worries their parents).

59.20 A more focused survey of United States teenagers aged 12 to 17, and their parents, was conducted in 2006 to examine how teenagers manage their online identities and personal information when using online social networks.[21] Some of the key findings of the survey were:

- 93% of American teenagers use the internet (increased from 87% in 2004), and 55% of them have online profiles.

---

18 Ibid, 2.

19 Greenburg Quinlan Rosner and Polimetrix, *Youth Monitor: Coming of Age in America* (2005), 1. See in particular *Part IV—The MySpace Generation* (2006).

20 Greenburg Quinlan Rosner and Polimetrix, *Youth Monitor: Coming of Age in America Part IV—The MySpace Generation* (2006), 1912.

21 A Lenhart and M Madden, *Teens, Privacy & Online Social Networks* (2007) Pew Internet & American Life Project.

- 66% of the teenagers with online profiles indicate they limit access to the profile in some way.

- 82% of teenagers with online profiles include their first name, and 79% have photos of themselves. Varying percentages include information such as the name of the city or town (61%), the name of their school (49%), email address (29%), last names (29%) and mobile phone numbers (2%).

- Boys are more likely than girls to post false information, which can be for privacy reasons but also to be playful or silly, and older teens are more likely than younger teens to disclose more personal information.

- 41% of teenagers accessing the online environment believe their online activity is monitored by their parents (an increase from 33% in 2004), while 65% of parents reported monitoring of their teenager's online activity.

59.21 One of the key questions the survey tried to answer was, 'Are today's teens less concerned about their privacy because the internet gives them so many opportunities to socialize and share information?'. The researchers found that

> there was a wide range of views among teens about privacy and disclosure of personal information. Whether in an online or offline context, teenagers do not fall neatly into clear-cut groups when it comes to their willingness to disclose information or the way they restrict access to the information that they do share. For most teens, decisions about privacy and disclosure depend on the nature of the encounter and their own personal circumstances. Teen decisions about whether to disclose or not involve questions like these: Do you live in a small town or big city? How did you create your network of online 'friends'? How old are you? Are you male or female? Do your parents have lots of rules about internet use? Do your parents view your profile? All these questions and more inform the decisions that teens make about how they present themselves online. Many, but not all, teens are aware of the risks of putting information online in a public and durable environment. Many, but certainly not all, teens make thoughtful choices about what to share in what context.[22]

59.22 There also appear to be differing standards depending upon the type of privacy under consideration. In a United States poll, the government's policy of eavesdropping on suspected terrorists' phone calls and emails without a warrant was considered wrong by 56% of 18–29 year olds (compared to 53% of 50–64 year olds who said it was the right thing to do).[23] Those young people criticising government surveillance include some who otherwise share intimate details in the online environment. It may seem illogical to be blasé about one kind of privacy but adamant about protecting another. The distinction, however, seems to be based upon control of the flow of

---

22 Ibid, iv.

23 J Berton, 'The Age of Privacy: Gen Y Not Shy Sharing Online—But Worries About Spying', *San Francisco Chronicle* (online), 20 May 2006, <www.sfgate.com>.

information. According to one young adult, 'what I get concerned about is when that control gets compromised without my consent'.[24]

ALRC consultations with young people

59.23 Given the paucity of literature on the attitudes of Australian young people to privacy, the ALRC determined there is a need to see if similar attitudes to those identified overseas prevail in Australia. The usual consultation and submission process undertaken by the ALRC does not preclude the participation of young people. Experience indicates, however, that young people do not traditionally engage in these processes without specific prompting. To complement other consultation initiatives undertaken in this Inquiry to reach a wider cohort of Australians,[25] the ALRC developed a number of processes particularly aimed at young people.

Talking Privacy website

59.24 In early 2007, the ALRC developed a website called 'Talking Privacy', which is accessible from the ALRC's home page. Designed specifically to appeal to young people, the website contains information about the Privacy Inquiry, links to further information about privacy law, and encourages young people to send in comments to the ALRC about their privacy issues or experiences. The site also contains information aimed particularly at teachers and students considering law reform or privacy as part of a school curriculum.

59.25 The aim of the Talking Privacy website was to engage young people using a familiar and well-used medium. As at the end of July 2007, the front page of the website had received 3,277 hits. Only a small number of young people had taken the further step of submitting comments for consideration by the ALRC, but these were insightful and of interest to the Inquiry. One young submitter to the Inquiry said:

> Generation Y may be optimistic, but to say care-free is a stretch. We are concerned that people in authority may abuse our rights in regards to privacy. Concerns about privacy for people in my age bracket is primarily in relation to our developing autonomy from parental control. Thus issues such as medical problems, school issues, social issues, sexual matters, and especially issues involving police, are all privacy issues from Generation Y. I am not overly concerned about the government and privacy, it is more a matter of privacy in relation to my autonomy from my parents, and other authority figures, eg teachers.[26]

59.26 As a further step, an age indicator box was placed on all pages which allow people to submit a comment to the Privacy Inquiry via the ALRC websites. While

---

24 Ibid.
25 See the description of all consultation processes undertaken in this Inquiry in Chapter 1.
26 J Boggs, *Submission PR 245,* 8 March 2007.

optional, this indicator has been useful to determine if there is a difference between comments depending upon the age bracket of the submitter.

Youth workshops

59.27 As noted in Chapter 1, the ALRC held a number of public forums as part of the Inquiry. In addition, in order to ensure that the views of young people were captured as part of the consultation process, the ALRC developed a workshop format for young people aged 13 to 25. The workshop provided young people with an opportunity to discuss general issues about privacy, and to provide comments and views in relation to set case studies which raise privacy issues in contexts relevant to young people.

59.28 A trial youth workshop was conducted in Sydney with a group of Year 10 and 11 students from Dubbo College Senior Campus. Youth workshops were then conducted in Perth, Brisbane and Hobart.[27]

59.29 The two hour workshops varied in size from five to 20 participants, with a total of 44 participants. The age of the participants ranged from 15 to mid-20s. The workshops were generally well received by the participants and were effective in involving young people and capturing their views on the relevant issues. The ALRC intends to conduct further youth workshops following release of this Discussion Paper.

59.30 The outcomes of workshops held to date have indicated a consistency with the research and literature in this area. Young people are aware of privacy issues and have certain concerns about their privacy. The issues of concern to them, however, may not necessarily coincide with the issues of concern to older Australians. As could be expected, most of the issues of concern centred around their experiences, and focused on issues directly affecting them.

59.31 The issue of privacy of personal space was raised a number of times by young people. This mostly related to searches of bags and lockers, privacy within the home, and privacy of meeting places such as religious halls. Issues about public surveillance were rarely raised. However, as the ALRC Privacy Inquiry is focused on personal information rather than personal space, the personal space issues were not fleshed out further in the workshops.

59.32 The type of information which young people considered to be sensitive were consistent with the current definitions in the *Privacy Act*, including information about sexual orientation, political views, ethnicity and religion. Health information, and in particular mental health information, and criminal records were also considered to be sensitive personal information.

---

27 The Perth workshop was supported by the Western Australian Office for Children and Youth; Brisbane was supported by the TC Beirne School of Law, University of Queensland, and Hobart was supported by the Commissioner for Children, Tasmania.

59.33 The focus of much of the discussion on privacy was the ability for the individual to choose what information about themselves they should disclose, and to whom. There was also an assumption that disclosure of personal information to a person or body did not mean that the person or body could use the information for a different purpose. This assumption is consistent with the existing privacy principles and the proposed Unified Privacy Principles. It is also consistent with past consultations conducted by the New South Wales Commission for Children and Young People.[28] The Commission provided a quote from one young person which sums up a typical reaction to privacy: 'Privacy matters because it is up to me whether or not I share information and who I share it with'.

59.34 At the same time, most young people accepted that there are many situations where it is necessary to disclose information for a greater public good—including to employers, police and government. Young people considered, however, that there should be clear rules and limitations on when mandatory disclosure can take place. There were a range of views as to the appropriate extent of the limitations.

59.35 The issue that raised the most concern was the disclosure to parents and others of health information of a person under the age of 18. There was a sophisticated understanding of the competing issues: that is, the need to provide confidential medical advice to young people; the need to ensure the ongoing safety and well being of the young patient; the interests and responsibilities of parents; and the professional obligations of the medical professional. Generally, however, there was an expectation that any young person who sought medical advice on their own should be entitled to confidentiality on the part of the medical professional. There was general agreement that any decision by the medical professional to disclose the information to parents, other medical professionals, or other people, should first be discussed with the patient.

59.36 Young people also expected confidentiality from the counselling profession, including school counsellors. There was strong support for the proposition that counselling services should be confidential, except in very limited circumstances where it was necessary to disclose information for the safety and wellbeing of the young person. A number of young people indicated that their understanding and experience of school counselling services is that they are not confidential.

59.37 Another prominent issue in discussions was the taking, and online posting, of photographs. Many young people had personal experience of such situations, and most had practical responses to the issues. In general, young people thought that it was good practice to obtain consent before taking a photograph of a person and posting it on the internet. Where the photographer is working for financial gain, they should be required to get consent and 'share' some of the financial gains with the person in the

28 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

photograph. It was accepted, however, that it is impossible to get the consent of every person in every photograph, particularly where the photograph captures a number of people in a public place. Most considered the rules which are in place in certain public spaces which limit or prohibit the taking of photographs, such as swimming pools and swimming carnivals, to be sensible.

59.38 It was accepted that it is often difficult to stop individuals from posting unauthorised photographs. Some young people went so far as to say there is implied consent—if you pose for a photograph it may be posted on the internet. This suggestion gets a negative reaction from most older Australians, and is indicative of the way in which young people are developing different norms around the use of the internet for communication purposes. Despite acknowledging difficulties with archiving of sites and permanent removal of website content, most young people considered that an individual should be able to have a photograph removed from a website if they did not consent to its posting. This was seen as a suitable remedy, and more practical than putting laws in place to prevent the posting.

59.39 One noticeable feature of the youth workshops and the discussion concerning the online posting of photographs was the varying levels of understanding of the ramifications of online posting. While the younger participants were the most likely to have experience of posting, or to have been the subject of posting, their understanding of the possible privacy implications for themselves or their friends was more limited.

59.40 Other issues which have raised concerns among older audiences were not seen by young people as controversial. Government access to school records to verify compliance with Youth Allowance requirements was seen by most as appropriate and fair. Covert collection of personal information by website operators that is later used to send spam was seen as annoying but an everyday part of life, and more open to practical, technology-based solutions than legal remedies. In one workshop the proposed Health and Social Services Access Card was considered appropriate, although further detail around the limitations on how information on the card can be used was considered desirable. While some participants were concerned about the reach of recent anti-terrorism legislation, many others considered it appropriate and did not consider their own freedoms had been affected.

Submissions and other consultations

59.41 The ALRC made other efforts to include young people and consult with representatives of children and young people as part of its general consultation processes. Roundtables were held in Sydney and Melbourne with key representatives of children and young people's interests, with the Sydney roundtable also attended by a number of young people. Meetings were held with each of the children's commissioners in New South Wales, Queensland and Tasmania, and submissions were received from a number of youth representative bodies. Many aspects of the submissions and consultations focused on issues around decision making by individuals under the age of 18, and are addressed in detail in Chapter 60. A broader

range of submissions dealt with the particular issue of taking and online posting of photographs, and these are examined in more detail below.

59.42 The ALRC did not include general questions in IP 31 about young people's perceptions of privacy, and submissions did not address this broader issue. The Youth Affairs Council of Victoria (YACVic) indicated that while young people's privacy is protected well enough by law, effective protection relies on a range of factors.

> The issues that impact on the actual level of protection that an individual receives could include a lack of personal or community understanding about young people's rights to privacy; difficulties in accessing complaints mechanisms and the power imbalance between a young person and 'professional' often inherent in a situation in which a young person's personal information is being collected.
>
> YACVic believes that young people's privacy is protected well enough in law, but that a range of other measures can be put in place or initiatives taken in order to ensure young people enjoy the highest level of protection and are not disadvantaged.[29]

59.43 One of the areas on which the ALRC received comment in submissions and consultations was the potential for young people's use of technology to have an impact on the privacy of others. For instance, a number of Australian schools have recently clamped down on online posting of inappropriate material, including video footage of fights involving school pupils.[30] The ALRC heard complaints about pupils posting pictures and comments on sites encouraging sexual assaults against teachers.

59.44 Another major concern is bullying using technology which, because of the ability to have constant communication at any time of the day or night, has the potential to be even more serious than face to face bullying.[31] A United States survey has indicated that one in three teenagers using the internet say they have been targets of a range of annoying and potentially menacing online activities, including receiving threatening messages, having private emails forwarded without consent, having embarrassing pictures posted without permission, or having rumours spread about them online.[32]

---

29 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007.

30 E Bellamy, 'Schools Act to Stamp Out Technology Abuse', *The Canberra Times* (Canberra), 8 March 2007, 7.

31 M Campbell, 'The Impact of the Mobile Phone on Young People's Social Life' (Paper presented at Social Change in the 21st Century Conference, Queensland University of Technology, Brisbane, 28 October 2005), 5.

32 A Lenhart, *Data Memo: Cyberbullying and Teens* (2007) Pew Internet & American Life Project.

59.45 Mobile phones, which are used by a very high proportion of children and young people, often without parental supervision,[33] are considered to pose a particular privacy risk by exposing young people to non-stop contact. As the newer third generation (3G) handsets also provide access to the internet, there are further opportunities for children and young people to be exposed to competitions, quizzes and direct marketing strategies.[34] The incorporation of cameras and video cameras into mobile phones was also raised as a concern due to the ability to 'hide' the action of taking an image behind the accepted behaviour of holding a mobile phone to make a call or send a message.

59.46 The ALRC did not ask a question about online social networking in IP 31. This issue has, however, continued to receive attention in the media. The growth of Australian participants in online social networking led the ALRC to explore the issue in consultations with young people. As a result, the ALRC has decided there are privacy concerns around the practice, and that these need further consideration.

Online social networking

Privacy concerns about online social networking

59.47 The past few years has seen an explosion of academic papers, media articles and online postings discussing the phenomenon of social networking. Social networking sites—such as MySpace, Facebook and YouTube—provide a forum for young people to promote themselves, and share their thoughts and experiences with like-minded young people—whether located next door or on the other side of the globe. Profiles on such websites often include photographs and video images as well as text.

59.48 On the one hand, there is a recognition that the explosion in the use of social networking sites is part of a cultural shift in the way in which people interact with others. Until recently, the internet has been used primarily as a source of information, but is now used by many, and particularly by young people, as a means of communication and an important part of social relations.[35]

59.49 On the other hand, there are concerns that participants in online social networking may be exposing themselves to dangers such as commercial exploitation and sexual predation. Of particular concern to many is the disclosure of participants' personal information to a worldwide audience, and whether participants fully understand the consequences of this disclosure. All of these concerns are heightened

---

33 A 2005 survey reported that mobile phone use was increasing in Australia, with one quarter of children aged 8 to 13 using a mobile phone regularly, and one third of parents of children in this age group reporting total lack of involvement with their child's use of mobile phones: Netratings Australian Pty Ltd, *kidsonline@home: Internet Use in Australian Homes [prepared for Australian Broadcasting Authority and NetAlert Limited]* (2005).

34 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007; Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.

35 J Wyn and others, *Young People, Wellbeing and Communication Technologies [Prepared for Victorian Health Promotion Foundation]* (2005) Youth Research Centre, University of Melbourne.

when discussing children and young people as participants in online social networking, due to their more limited capacity to understand the consequences.[36]

59.50 It should also be noted that not all online social networking is done by young people. MySpace Australia has three million members, 50% of whom are over the age of 25.[37] A survey of 2,000 working adults in the United States indicated that just under half participated in online social networking, and over half of these participants were over the age of 35.[38] Many companies and individuals seeking to promote themselves in the online world now participate in key online social networks. For example, following the lead of presidential candidates in the United States, Australian politicians are being encouraged to develop their own MySpace profiles to engage better with younger voters.[39] There is also a growing number of social networking sites aimed at children as young as 6 or 7.[40]

59.51 There is, however, evidence to suggest that young people use the social networking sites differently to older people. In 2007, market research company YouGov undertook research in the United Kingdom on behalf of social network Viadeo to find out what kind of personal information people place online.[41] The results of the survey of adults showed that those in the 18–24 year old group were more likely to post information about themselves than those in older age groups. Interestingly, 54% of 18–24 year olds indicated that others had posted information about them with or without their consent. This all contributes to what is called a person's 'NetRep', a personal online brand, that others contribute to whether we like it or not.

59.52 Online social networking throws up two issues for consideration. The first is young people choosing to disclose information about themselves. This chapter focuses on this issue. The second issue surrounding personal information on social networking sites is the ability for third parties to post, alter or remove personal information about another. This issue is discussed below in relation to photographs, and also in Chapter 8.

---

36 See Ch 60 for a discussion on decision-making capacity and brain development of children and young people.

37 A Moses, 'Pollies Chase the Youth Vote on MySpace', *Sydney Morning Herald* (online), 29 May 2007, <www.smh.com.au>.

38 'Social Networkers Disclose Too Much Personal Info, Says CA', *OUT-LAW* (online), 9 October 2006, <www.out-law.com>.

39 A Moses, 'Pollies Chase the Youth Vote on MySpace', *Sydney Morning Herald* (online), 29 May 2007, <www.smh.com.au>; C Walters, 'Kevin, 49, Seeks Friends He Can Count', *Sydney Morning Herald* (online), 13 July 2007, <www.smh.com.au>.

40 'It's Like MySpace, But With Training Wheels', *Sydney Morning Herald* (online), 13 July 2007, <www.smh.com.au>.

41 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007).

Choosing to disclose

59.53 Many commentators (and parents) have lamented the fact that young people post large amounts of detailed personal information about themselves on websites. This is the first generation to have their 'sexual adventures, drug taking, immature opinions and personal photographs … indelibly recorded electronically'.[42] It has become a typical way in which young people can explore their identities, and regularly post personal musings, philosophies and opinions as well as more prosaic descriptions of everyday events and the latest snapshots of themselves and friends.[43]

59.54 This does not, however, mean that young people do not value privacy. As has been found in many surveys and the ALRC's own consultations, young people do value the right to privacy but they also value the right to choose to disclose information about themselves. A recent United States study of teen use of social networks, which focused on privacy issues, found that many teenagers appear more privacy savvy than commentators may have thought.

> Most teenagers are taking steps to protect themselves from the most obvious areas of risk. The new survey shows that many youth actively manage their personal information as they perform a balancing act between keeping some important pieces of information confined to their network of trusted friends and, at the same time, participating in a new, exciting process of creating content for their profiles and making new friends. Most teens believe some information seems acceptable—even desirable—to share, while other information needs to be protected.[44]

59.55 As noted above, the ability to control the disclosure of personal information is seen as an important element of the respect for privacy. This concern about control is reflected in the reaction of members of the popular social networking site Facebook when the site introduced a feature automatically broadcasting changes made to a member's profile.[45] Facebook is predicated on controlling the privacy of your profile by determining who can see your profile, ie, who can be your 'friend'. Even though the changes to member profiles were only automatically broadcast to those listed as 'friends', there was a huge backlash from members who threatened to boycott the site. Facebook hastily added controls so that members can choose to hide profile changes. It seems that young people will consider what information they share depending upon the rules of the community, and changing the rules of the community, or changing the membership of the community, may lead to a breach of privacy. Facebook's chief privacy officer, Chris Kelly, has been quoted as saying that the classic notion of the

---

42 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

43 J Wyn and others, *Young People, Wellbeing and Communication Technologies [Prepared for Victorian Health Promotion Foundation]* (2005) Youth Research Centre, University of Melbourne, 14–17.

44 A Lenhart and M Madden, *Teens, Privacy & Online Social Networks* (2007) Pew Internet & American Life Project, i–ii.

45 K Coughlin, 'Facebook's Facelife Uncovers What Many See as Flaws: Social Networking Sites' Mainstream Aspirations are Turning Off Purists', *Times-Picayune* (online), 5 November 2006, <www.timespicayune.com>.

right of privacy as the right 'to be left alone' has changed to the notion of 'I want control over my information'.[46]

59.56 Some have noted that, while the right to choose to disclose is important, there is also a need to be able to change your mind.[47] The medium in which social networks are contained, however, does not make it easy to change your mind, and we are only just beginning to see what some of the consequences for later life choices might be.

> The potential harm from out-of-date, conflicting and inaccurate information on the Web is amplified by the fact that internet search engines such as Google store or cache Webpages which makes the information available online even after the author has removed the information in question. This makes it very difficult to remove or correct wrong or compromising information, which could be harmful to a person's career chances.[48]

59.57 The 2007 survey by YouGov, noted above, also asked recruitment managers and directors whether they are using personal information on websites to inform recruitment decisions. While only 18% of the respondents indicated they had found information online about a prospective employee, 59% of those said it had impacted on their decision whether to employ the person, including 15% having a negative impact as a result of the online information.[49] Media stories are beginning to emerge of people who have lost job opportunities as a result of their earlier online disclosures,[50] and some of the young people consulted by the ALRC reported disciplinary outcomes as a consequence of their online activity.

59.58 There are also safety concerns about disclosing personal information in a public space. Just as chat rooms have been a concern in the past, there are now concerns that social networking sites are being used by sexual predators. Two New South Wales Members of Parliament have proposed laws banning convicted sex offenders from internet chat rooms and social networking sites, although the mechanism for achieving this is still under consideration.[51] Young people are generally well rehearsed on the 'stranger danger' elements of online activity in chat rooms, but the ALRC consultations indicated that not all young people have got the message that the world of social networking is a public one, and holds safety traps and pitfalls.

---

46 'Facebook Banks on Privacy', *Sydney Morning Herald* (online), 16 July 2007, <www.smh.com.au>.

47 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

48 YouGov, *What Does Your NetRep Say About You? [Research Commissioned by Viadeo]* (2007), 6.

49 Ibid, 4.

50 See, eg, M Mann, 'Some Job Hunters are What They Post', *National Law Journal* (online), 9 May 2007, <www.law.com>.

51 'Ban Sex Offenders from Chat Sites: Opposition', *Sydney Morning Herald* (online), 27 May 2007, <www.smh.com.au>.

Regulatory options

59.59 Concerns about the dangers and possible adverse consequences for children and young people using social networking sites has led to consideration by some legislators and commentators of appropriate regulatory options to eliminate, or at least alleviate, the concerns.

59.60 It should be noted that many of the social networking sites already build in some age restrictions as a condition of joining their online network. For example, the most popular social networking site, MySpace, requires users to be aged 14 or over. The terms and conditions specify that profiles of members believed to be under 14 years of age may be deleted,[52] and many of the tips to users and parents encourage reporting of under-age profiles. Facebook was originally only open to high school and college students, but is now open to any high school or college student aged 13 to 17, or any person over the age of 18. The terms of entry to the site specify that profiles of under-age users may be deleted.[53]

59.61 As described in Chapter 60, the *Children's Online Privacy Protection Act* (US) (COPPA) applies to operators of commercial websites and online services directed to children under the age of 13 that collect personal information from children, and to operators of general websites with 'actual knowledge' that they are collecting information from children under the age of 13. One of the requirements is for website operators to provide notice to parents and obtain verifiable parental consent before collecting personal information of a child under the age of 13. The Federal Trade Commission (FTC), which enforces COPPA, has a sliding scale approach to obtaining verifiable parental consent, with the requirements for obtaining consent more rigorous where the intended use of the information involves disclosure to third parties rather than internal use. Where the information is to be used for internal purposes only, verifiable parental consent can be obtained through the use of an email message to the parent, coupled with additional steps to provide assurances that the person providing the consent is, in fact, the parent. More rigorous methods specified include: fax- or mail-back forms; credit card transactions; staffed toll-free numbers; digital certificates using public key technology; and emails accompanied by Personal Identification Numbers or passwords. While generally COPPA has been considered a successful measure,[54] there has been criticism that the age verification mechanisms are easy to circumvent.[55]

---

52 MySpace, *MySpace.com Terms of Use Agreement* (2007) <www.myspace.com> at 31 July 2007.

53 Facebook, *Terms of Use* (2007) <www.facebook.com> at 31 July 2007.

54 See discussion in Chapter 60.

55 M Hersh, 'Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet' (2001) 28 *Fordham Urban Law Journal* 1831, 1870.

59.62 It has been suggested that using something like COPPA, with a higher age barrier, would be an appropriate way to regulate social networking sites.[56] COPPA has already been used to alter the practices of social networking site Xanga.com, which was penalised US$1 million for collecting, using and disclosing personal information from children under the age of 13 without first notifying parents and obtaining their consent. In order to comply with COPPA, it is common practice of United States and many other international social networking sites to ask participants to check a box certifying they are 13 years or older before they can create a profile and, as noted above, some have voluntarily set the age barrier higher. Xanga.com included such a check box, but then allowed users under the age of 13 to create a profile with clarification of their age status. The consent order imposed on Xanga.com by the FTC, which sets out steps to be taken to comply with COPPA, is considered to be 'best practice' for social networking sites.[57] It includes a requirement to place links to information about protecting children's online privacy in privacy policies on websites, any information collection point on websites and in notices sent directly to parents.

59.63 A number of legislators in the United States have proposed protective measures aimed at prohibiting or limiting access by young people to social networking sites. The proposed Deleting Online Predators Act 2007 is presently before the United States Congress, and seeks to prohibit student access to social networking sites in schools and libraries unless under adult supervision. A number of states in the United States have passed or proposed laws requiring social networking website operators to verify the age of every user; requiring parental permission for those under the age of 18. The effectiveness of the proposals has been questioned given the absence of effective online age verification mechanisms.[58] To provide any form of protection, the verification mechanism must involve more than an assumption that the user is honestly disclosing his or her age.[59]

59.64 There is also a question as to whether stopping young people from engaging in online social networking is the most appropriate regulatory approach. These networks have become an integral part of the way that young people express themselves and communicate with each other.

---

56 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

57 *Consent Decree and Order for Civil Penalties, Injunction and Other Relief—United States v Xanga.com*, September 2006; R Urbach, 'FTC Tackles Social Networking', *DMNews* (online), 21 November 2006, <www.dmnews.com>.

58 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

59 Age verification and parental consent verification mechanisms are further discussed in Ch 60.

> Before we can solve the social networking dilemma, we must first grasp the cultural nuances of virtual communities and the potential implications of any new proposals. Otherwise, our rush to respond may fail to fully address those important concerns.[60]

The need for education

59.65 In contrast to a regulatory mechanism, others have highlighted the need for education of students to inform them of the possible pitfalls in sharing information online.[61] The need for education is supported by the reported reaction of many young people when they are informed that schools, police, parents and employers may be reading their online profiles. It has been suggested that they do not think of the internet as a public place, or that their personal profile is a highly accessible, public document.[62] Even where sites provide privacy control options for profiles (and many do), many young people choose a public profile in order to maximise their potential for making friends, not necessarily understanding the reality of what it means to be 'public' on the internet. Others are knowingly using social networking sites for self-promotion—but again some question whether that self-promotion is undertaken with a full, mature understanding of the consequences. As one commentator has noted, 'the teenagers chattering away online are media literate, but they are not media wise'.[63]

59.66 American academics Dr Ilene Berson and Dr Michael Berson have written extensively on the protection of children's privacy in the digital age. They note that children today are often the subject of parental publishing of their life experiences from birth, and from quite young ages learn to interact in digital spaces. The proliferation of online personal information, however, has also desensitised young people, and they remain oblivious to ways to maximise privacy in their online activities.[64] Berson and Berson discuss the need to teach all young people 'digital literacy', a concept which

> emphasizes the capacity to fully participate as a responsible member of a technologically engaged society and refers to the skills that people need to understand and constructively navigate the digital media that surrounds them. It addresses safety and security while fostering broader preparation for digitized and networked environments.[65]

59.67 Berson and Berson note that it is essential to teach digital literacy, as while young people are often proficient in using the tools of the digital world, 'they have typically not acquired the proficiency to function responsibly as members of networked

---

60 H Valetk, 'Playing with Privacy: Virtual Communities Raise New Questions', *Law.com* (online), 24 May 2007, <www.law.com>.

61 See, eg, S Steinbach and L Deavers, 'The Brave New World of MySpace and Facebook', *Inside Higher Ed* (online), 3 April 2007, <insidehighered.com>.

62 C Thomas, 'Kids Think Posting Online is Private, Say Educators', *Hamilton Spectator* (online), 1 May 2007, <www.hamiltonspectator.com>; S Steinbach and L Deavers, 'The Brave New World of MySpace and Facebook', *Inside Higher Ed* (online), 3 April 2007, <insidehighered.com>.

63 P Bazalgette, 'Your Honour, It's About Those Facebook Photos of You at 20 ...' *The Observer* (online), 20 May 2007, <observer.guardian.co.uk>.

64 I Berson and M Berson, 'Children and Their Digital Dossiers: Lesson in Privacy Right in the Digital Age' (2006) 21 *International Journal of Social Education* 135, 141.

65 Ibid, 142.

communities'.[66] An important element of learning to apply critical analysis skills and make ethical decisions in this environment is to control disclosure of personal information. At present, as many parents are themselves either unable to operate, or inexperienced at operating, in this environment, most of these skills are being learned from the young person's peers. While it is clear that the technical skills are being learned, it is questionable whether the decision-making skills are developed effectively before too many mistakes are made.

Photographs and other images

Background

59.68 One of the key issues that arose in consultations with young people is the regulation of unauthorised photographs. The accessibility and uptake of social networking sites has led to increased posting of photographs and video footage by individuals, and some of the concerns about privacy and social networking are linked to concerns about posting of online photographs and videos. The concerns, however, go beyond the use of photographs and other images on social networking sites.

59.69 The *Privacy Act* protects personal information that is held, or collected for inclusion, in a 'record'. A 'record' is defined to include a photograph or other pictorial representation of a person.[67] Thus, if an individual's identity is apparent, or can reasonably be ascertained, from a photograph or other image, then the collection, use and disclosure of that image is covered by the *Privacy Act*. This extends to video images as well as still photographs. The rest of this chapter uses the term 'image' to cover photographs and moving images. All of the privacy principles applicable to the collection and disclosure of personal information will also apply to the taking and publication of images.

59.70 As with other forms of personal information, the coverage of images is limited by the scope of the *Privacy Act.* For example, an image is not covered by the *Privacy Act* if it was taken by an individual who is acting in their private capacity. The image is also not covered if the image was taken by someone acting on behalf of a small business.[68] Similarly, images taken by a person acting on behalf of a state or territory agency are not covered by the *Privacy Act*, although they may be covered by a similar state or territory law.[69]

---

66 Ibid, 142.

67 *Privacy Act 1988* (Cth) s 6. For more detailed discussion of the definitions of 'record' and 'personal information', see Ch 3.

68 Although see Proposal 35–1 which seeks to bring small business under the coverage of the *Privacy Act*.

69 See Ch 2 for an overview of applicable state and territory privacy laws and the ALRC's proposals in Ch 4 for introduction of harmonised privacy laws.

59.71 The taking of images without consent has raised significant concerns in the past few years. While the issues are not limited to images of children and young people, many of the examples have related to children and young people. These have included: the taking of photographs of young male rowers and footballers and posting them on a website containing links to what the media described as a 'gay website'; discovery of a website containing hundreds of images of children taken at recreational sites in Queensland, and thought to be used for sexual gratification; and examples of 'upskirting'—the covert taking of photographs underneath clothing—in a number of public places.[70]

59.72 Mobile phone cameras and mobile phone video cameras seem to have heightened these concerns, due to their small size and increasing availability in the community. However, the issues of unauthorised taking of images extends beyond any one type of technology. One author has noted that concerns about covert taking of photographs have existed since the 1890s, and reappeared on a regular basis as different forms of cameras became available.[71] Most recently, the concerns about unauthorised images have exploded with the ease and open accessibility of online publication. The issues are the same, however, regardless of the medium of publication.

59.73 Community concerns have led the Standing Committee of Attorneys-General (SCAG) to consider the issue. A discussion paper released for public comment in August 2005 set out the concerns and raised a number of options for reform.[72] While the paper was particularly focused on the posting of unauthorised photographs on the internet, much of the discussion addressed the issue of taking photographs generally. The SCAG discussion paper includes extensive comment on the issue of giving consent to the taking of a photograph. The discussion paper notes that the absence of consent may affect whether the taking of a photograph is considered to be unauthorised and, if consent was obtained, whether the subsequent use is connected with any consent that was given at the time the photograph was taken.[73] The issue continues to be discussed in SCAG, with some jurisdictions pushing for uniform criminal laws.[74]

---

70 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), 5.

71 C Ludlow, '"The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135, 137. See also Australian Mobile Telecommunications Association, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, October 2005. The seminal article on privacy was prompted by advances in photographic technology: S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

72 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005). For an overview of some of the examples that have led to consideration of the issue, see [7]–[18].

73 See, eg, Ibid, [31]–[38].

74 K Ngyuen, 'Law Chiefs have their Eyes on Voyeurs', *The Age* (online), 28 July 2006, <www.theage .com.au>.

59.74 The Victorian Law Reform Commission has also commenced an inquiry on surveillance in public places. It is expected that a number of issues concerning the taking and use of unauthorised photographs will arise in that inquiry. The Victorian Law Reform Commission is planning to release a consultation paper on the inquiry later in 2007.

Submissions and consultations

59.75 A number of submissions raised concerns about the lack of clarity of the existing law in relation to photographing children. A number of stakeholders expressed particular concern about the ease of taking and disseminating photographic images using mobile technology.[75]

59.76 The need to safeguard the safety and privacy of children from people with no legitimate purpose for taking and publishing photos was highlighted.[76] The ALRC was presented with evidence about the harm that can be done to children where they are the victims of using photographs for sexual gratification, even where the photograph itself was not sexually explicit in nature.[77] One caller to the ALRC indicated that the fear and insecurity of not knowing how photographs will be used has led to changes in community behaviour, and an intolerance towards strangers taking photographs around children. The Queensland Commission for Children and Young People and Child Guardian indicated that it regularly receives phone calls from concerned parents, managers of sporting associations and others who believe it is against the law to take photos of children at events.[78] One submitter lamented that this is the 're-engineering of society by stealth and misinformation'.[79] The Office of the Privacy Commissioner considered that developing social protocols that make it acceptable to ask a person to refrain from using a camera on a beach or outside of a school is a positive step.[80]

59.77 The issues around unauthorised images are not limited to safety concerns about children and young people. As noted above, the ALRC's consultations with young people indicated that the online publication of images without the consent of the subject of the photograph is a common occurrence—whether the image itself was taken with or without the subject's consent. The posting itself was taken for granted by some, and the ease of its publication accepted as a reality by most. While the posting may not

---

75 See, eg, Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007.

76 Queensland Police Service, *Submission PR 222,* 9 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007;

77 Queensland Police Service, *Submission PR 222,* 9 March 2007.

78 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

79 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

80 Office of the Privacy Commissioner, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Use of Photographs on the Internet and Related Privacy Issues*, November 2005.

be criminal in nature, the possible consequences of unauthorised posting can include bullying, ridicule, embarrassment and generally a breach of privacy.

59.78 Overall, concerns about taking and using unauthorised images, particularly of children, led some to consider the need for stricter regulation.

> Sadly, there is now good reason for the existence of clear guidance through the Privacy Act governing limitations on the broadcasting of identifying images of children, restricting the ability of organisations to publicly display a photo of a child in their care, without the express consent of the parent or guardian.[81]

59.79 Generally, however, there was not widespread support for a blanket ban on taking of images of children without express consent. Instead, there were calls for a clearer regime which balances effectively the need to protect children from exploitation for sexual and commercial purposes with the need not to place undue restrictions on the taking of images by parents, family and friends.[82] While there are some individuals who offend others through inappropriate behaviour, these are in the minority and the vast majority of appropriate users should not be restricted from using photography in appropriate ways.[83] Some considered that privacy laws are an appropriate method for regulating this issue.[84]

59.80 In contrast, the Arts Law Centre of Australia was opposed to any law which requires photographers or documentary filmmakers to obtain the consent of individuals before taking a photograph or film footage.[85] The concerns of the artistic community in relation to privacy laws preventing use of a person's image are addressed in more detail in Chapter 5.

Options for reform

59.81 In the SCAG discussion paper on unauthorised photographs, a number of reform options were discussed:

- possible criminal offences regarding unauthorised use of photographs of children;

---

81 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

82 Queensland Police Service, *Submission PR 222,* 9 March 2007; Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007.

83 Australian Mobile Telecommunications Association, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, October 2005.

84 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

85 Arts Law Centre of Australia, *Submission PR 125,* 15 January 2007. See also National Association for the Visual Arts, *Submission PR 151,* 30 January 2007.

- take down provisions for online content;
- possible civil rights regarding unauthorised publication of images of people; and
- education campaigns.

Criminal law

59.82 There are a number of existing criminal laws that address the taking and use of unauthorised images for offensive purposes. Some of these include:

- use of surveillance devices to record a 'private activity' without consent;[86]
- filming for indecent purposes;[87]
- making an image of a child engaged in a private act for prurient purposes;[88]
- making indecent visual images of a child under the age of 16;[89]
- committing indecent or offensive acts in a public place;[90]
- child pornography offences;[91] and
- using a telecommunications network or carriage service to facilitate certain offences.[92]

59.83 There is concern that a number of new activities involving taking and publication of images are not covered by existing criminal offences. A combination of offences, such as stalking, using optical devices without consent and indecent behaviour, have been used successfully to prosecute instances of crimes such as

---

86 See, eg, *Surveillance Devices Act 1999* (Vic) ss 6–7; *Surveillance Devices Act 2000* (NT) s 5; *Surveillance Devices Act 1998* (WA) ss 5–6. Not all of the surveillance devices legislation in Australia, however, has a general prohibition on the use of surveillance devices without authorisation or consent: see, eg, in South Australia the prohibition is limited to listening devices: *Listening and Surveillance Devices Act 1972* (SA) s 4.

87 See, eg, *Summary Offences Act 1988* (NSW) pt 3B. In some jurisdictions, however, the offence only applies where the indecent material is produced for the purpose of sale: see, eg, *Summary Offences Act 1953* (Qld) pt 7.

88 See, eg, *Criminal Law Consolidation Act 1935* (SA) s 63B.

89 See, eg, *Criminal Code* (Qld) s 210(1)(f)

90 See, eg, Ibid s 227(1); *Summary Offences Act 1988* (NSW) s 4; *Police Offences Act 1935* (Tas) s 13.

91 See, eg, *Crimes Act 1958* (Vic) pt 1 div 13; *Criminal Code Act 1924* (Tas) ss 130–130G.

92 See, eg, *Criminal Code* (Cth) s 474.14 (using a telcommunications network to commit a serious offence); s 474.17 (using a carriage service to menace, harass or cause offence); ss 474.19–474.20 (using a carriage service to intentionally access, transmit or make available child pornography material); ss 474.22–474.23 (using a carriage service to intentionally access, transmit or make available child abuse material).

'upskirting'. While acknowledging that 'upskirting' conduct could be, and has been, successfully prosecuted using existing criminal offences, the Victorian Attorney-General will introduce a bill to the Victorian Parliament to criminalise specifically the act of photographing up a woman's skirt without her knowledge, and to ban the distribution of such images by email or SMS.[93]

59.84 As noted in the SCAG discussion paper, a number of situations of concern do not fit neatly into the existing laws. Most of the criminal offences involve elements of 'private activity' or a 'private act', so that any activity carried out in a public environment, or at least an act which is not considered an act where you would expect to be afforded privacy—such as rowing, or playing in a public playground—is not covered by the particular offence. There is therefore a question of whether criminal offences should extend to the making of images without consent in any public or private situation where the purpose for making the image is to provide for sexual arousal or sexual gratification.

59.85 Another concern that has been raised is that a number of the criminal offences in the states and territories do not cover images of children that are not sexually explicit in nature, but that may be used for purposes of sexual gratification. The Queensland Police Service provided the ALRC with a number of case studies involving images of children in socially appropriate situations and attire that had been taken and used for sexual gratification.[94] Due to the existing definitions of 'child exploitation material', 'child abuse material' and 'child pornography' material in Commonwealth and Queensland legislation, the Police have had only limited success in prosecuting the individuals involved, and even greater difficulties in having the images removed from the internet as they were not considered to be offensive content.

59.86 One suggestion is to have a wider offence which is not restricted to private acts, but covers the taking or publication of an image where the use or intended use is one which a reasonable adult would find exploitative or offensive, or the use or intended use was for the purpose of sexual gratification.[95] While some of the suggestions have been limited to images of children under a set age, an expansion of the offence to cover images of adults taken or used without consent could be considered.[96] Expanding the offence to include what a reasonable adult would find exploitative or offensive would be a significant step, and further consideration would need to be given to the kind of

---

93 'Updated Laws to Tackle "Upskirting" Photos', *Sydney Morning Herald* (online), 27 May 2007, <www.smh.com.au>.

94 Queensland Police Service, *Submission PR 222,* 9 March 2007.

95 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), 33. A similar suggestion was made by Queensland Police Service, *Submission PR 222,* 9 March 2007.

96 A 'voyeurism' offence applicable to adults was suggested in the SCAG discussion paper, but was limited to situations where there was an expectation of privacy, similar to the NSW offence: Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), 34.

uses that might be captured by such a formula, and whether it is appropriate to ascribe criminal conduct to these uses.

59.87 It is clear that there are gaps in the existing criminal law and not all inappropriate conduct relating to the taking and use of unauthorised images is presently covered in all jurisdictions.[97] As this Inquiry is focused on the *Privacy Act* and related privacy laws, the ALRC will not focus on the gaps in the criminal law. It is expected that this issue will receive further attention within SCAG. The ALRC notes, however, that the submissions made to, and the consultations held, in this Inquiry have not expressed support for making it a criminal offence to take an image of a child or an adult without consent. Any proposed criminal offences should not be unduly restrictive and must still provide for family, friends, community bodies, schools, media, the artistic community and others to take and publish appropriate images.

Take down notices for online content

59.88 In consultations with young people, the ability to have unauthorised internet content removed upon request was considered an appropriate and practical remedy.

59.89 Chapter 8 describes the co-regulatory scheme administered by the Australian Communications and Media Authority (ACMA) for the regulation of internet content.[98] As indicated in that chapter, the scheme is dependent on the *National Classification Code* and decisions of the Classification Board to determine what is prohibited content that can be the subject of a take down notice.

59.90 Chapter 8 also asks a question about whether the take down notice scheme should be expanded beyond the existing definitions of prohibited content, and possibly allow for an additional circumstance where the content may constitute an invasion of an individual's privacy. Such a remedy would be useful for removing unauthorised images from the internet where a breach of privacy existed. As noted in the chapter, however, such a move would be likely to be opposed by some with an interest in maintaining freedom of expression in the online environment. The ALRC will consult on this issue further before completion of the final Report.

Civil rights

59.91 It has already been noted above that the community in general does not support a complete ban on the taking of images without consent. Neither does the ALRC consider this to be a viable option for reform. There are valid concerns, however, that

---

97 For a good overview of the existing laws and the limitations of each, see Ibid, app 1.

98 The online regulation scheme is at present set out in *Broadcasting Services Act 1992* (Cth) sch 5, although it is proposed to be expanded by the Communications Legislation Amendment (Content Services) Bill 2007 to cover live streamed content services, mobile phone-based services and services that provide links to content, and to move the entire scheme to a new sch 7 of the Act.

there are some types of publication that may not be criminal in nature, but still affect an individual's privacy interests.

59.92 The SCAG discussion paper looked at the use of copyright law enacted in The Netherlands to eradicate the trade in video recordings showing children on beaches and nudist beaches where the recording is made without the parents' or child's consent.[99] As part of the civil response to the issue, the *Copyright Act 1912* (Netherlands) was amended to provide that the publication of a photographic or video portrait made without a commission is not permitted if this would be contrary to the reasonable interests of the person shown in the photograph or video. The Act provides that a child or his or her legal representative may apply to the courts for an injunction to restrain publication. A number of submissions made in response to the SCAG discussion paper supported this kind of 'reasonable interests' approach, but questioned whether amendment to Australian copyright law was the best response.[100]

59.93 Chapter 5 of this paper gives detailed consideration to the introduction of a statutory cause of action for invasion of privacy. The ALRC, supporting a proposal of the New South Wales Law Reform Commission, proposes the introduction of such a cause of action to protect individuals from unwanted intrusions into their private lives or affairs in a broad range of contexts. This will include publication of images that are considered to be an invasion of privacy.

59.94 Chapter 5 also discusses the proposed elements for the cause of action. To fall within a definition of what is considered 'private', there must be both a reasonable expectation of privacy in all the circumstances, and the act complained of must be, in all the circumstances, sufficiently serious to cause substantial offence to a person of ordinary sensibilities. There are also a number of proposed defences to the cause of action, including where the information disclosed was a matter of public interest or was a fair comment on a matter of public interest. A wide range of remedies is also proposed.

59.95 The ALRC considers that appropriate implementation of the statutory cause of action will capture a range of activities relating to the publication of images which are currently considered to be inappropriate, but unregulated. This includes online publication by individuals of images taken, or at least published, without consent where there is an invasion of personal privacy.

59.96 It is not expected that every invasion of privacy will be pursued through the courts. As discussed in Chapter 5, however, the introduction of a cause of action,

---

99 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005) citing *Convention on the Rights of the Child: Initial Reports of States Parties Due in 1997: Netherlands: Addendum*, CRC/C/51/Add.1 (1997).

100 See, eg, New South Wales Commission for Children and Young People, *Submission to the Standing Committee of Attorneys-General Discussion Paper Unauthorised Use of Photographs on the Internet and Ancillary Privacy Issues*, October 2005.

accompanied by appropriate information made available to the public, is likely to raise consciousness within the community and assist with the development of appropriate standards of behaviour.

Conditional rights

59.97 Many bodies have begun to include as part of conditions of entry to premises, or participation in an event, that cameras, video cameras or mobile phones incorporating cameras or video cameras, are not to be brought onto the premises or used. This has become typical in change rooms and private gyms, where people expect an element of privacy, but has been more controversial when applied to public events and places such as life saving and sports carnivals, or public swimming pools.[101]

59.98 The ALRC is not making any proposals about banning or restricting the taking of images in such places. Decisions regarding imposing such conditions of entry or participation should be left to the bodies owning the premises or organising the events. The ALRC notes, however, the general opposition in the community to a complete ban on photography in public places, as well as the concerns about protection of privacy, and in particular the protection of children. These attitudes need to be balanced appropriately in making such decisions.

Education

59.99 The activity of taking images appears to many members of the community to be under siege. Conversely, others have concerns about guaranteeing the privacy and safety of children in the community. Clearly there is confusion as to what is acceptable, what is legal, and when inappropriate behaviour can be stopped or punished. It is also an area where community attitudes and behaviours are changing.

59.100 There is a need for further information to be made available to the community to clarify the laws in this area. The Privacy Commissioner of Victoria has published a fact sheet on mobile phones with cameras covering many of the issues of concern and the legal protections in place.[102] The Queensland Commissioner for Children and Young People and Child Guardian is developing a similar fact sheet on photography and video footage, with a particular emphasis on children's and young people's right to privacy. This kind of information needs to be more readily available in order to educate the community, provide information on what is appropriate and inappropriate behaviour, inform the public about available remedies, and facilitate an informed debate about future law reform in this area.

---

101 R Grayson, 'No Right Not to Be Photographed—Councils Overreact', *On Line Opinion* (online), 12 July 2005, <www.onlineopinion.com.au>.

102 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras—Info Sheet 05.03* (2003).

ALRC's view

An ongoing study of attitudes to privacy

59.101 The research and consultation undertaken by the ALRC in relation to the attitudes of children and young people to privacy suggest that the existing framework for the protection of personal information, reformed in accordance with the proposals of the ALRC in this Discussion Paper, adequately reflects the expectations of Australian young people. While young people have slightly different privacy concerns and experiences when compared to older Australians, the differences are not so great as to warrant a reconsideration of the basic framework of the *Privacy Act*. Many of the proposed changes to the framework aimed at greater clarity, national consistency and improved enforcement, however, will be of benefit to all Australians and in accordance with the expectations of young Australians.

59.102 The ALRC notes that there are differences in opinion among young people—and between young people and older Australians—on some issues related to privacy. A key example is the regulation of privacy issues in the online environment, with young people often able to recognise the practicalities and impracticalities of regulation in this environment due to their familiarity and ease with the use of the technology. Young people have suggested that individual control is a more viable regulatory option than technical legal solutions. Another area of interest is the level of acceptance of government interference with privacy rights in the name of the public good. While not unanimous in their support of government, many younger people were more open than many older Australians to accepting a certain level of curtailment of individual privacy.

59.103 These shifts in attitudes are to be expected as Australian society and the world around us continues to change. In undertaking the current Inquiry, the ALRC is mindful that the existing *Privacy Act* is largely based on a previous ALRC inquiry conducted in the late 1970s and early 1980s. The current Inquiry is being conducted in a very different world, where technology has greatly changed the way in which we hold and exchange information, governments have contracted out a wide range of services, and the threat of terrorism on Australian soil has placed security concerns high on the public agenda. In trying to gauge whether expectations of privacy law have changed, however, the ALRC had little Australian research to draw on.

59.104 As indicated in Chapter 7, even with the implementation of the ALRC's final recommendations for reform, the *Privacy Act* will continue to operate in a changing environment and would benefit from future review to ensure it continues to meet its objectives. Additionally, privacy impact assessments conducted by agencies and organisations will need to take into account current attitudes of Australians towards privacy and the acceptable level of interference with individual privacy. Any such review or assessment would be best made with the assistance of accurate and up-to-date data on community attitudes to privacy. It is the ALRC's preliminary view that the Australian Government fund a longitudinal study of the attitudes of Australians to

privacy. The study should be representative of the Australian population, and include participants under the age of 18.

59.105 As is noted above, the OPC has commissioned three surveys on community attitudes to privacy, and each was conducted by Roy Morgan Research: in 1994, 2001 and 2004.[103] The 2004 survey was a partial replication of the 2001 survey, and these were similar to, but not directly comparable with, the 1994 survey.[104] The surveys were quantitative in nature, involving telephone interviews with adult respondents representative of the adult population nationwide. While Roy Morgan undertook some qualitative research as part of the 2001 survey, there was no report on the outcome of that research.

59.106 These surveys have provided some useful information on community attitudes, but are not a substitute for a proper longitudinal study encompassing both quantitative and qualitative research. Qualitative research, while more difficult to conduct and analyse, is more likely to explain experiences and beliefs in terms of the wider contexts of peoples' lives. A longitudinal study will help to answer whether the attitudes of Generation Y today will persist over time, if they are attributable to youth more generally, and whether generations which follow will have different attitudes.

59.107 At this point, the ALRC does not consider that the OPC is the appropriate body to conduct, or even commission, a longitudinal study. It is appropriate, however, that the Australian Government provide funding for the project given that the outcomes will have direct relevance to national policy development.

59.108 It may be possible for researchers to obtain funding for a longitudinal privacy attitudes study through the Australian Research Council. Funding under the *Discovery Projects* scheme, for example, might suit this kind of project. It is noted, however, that an effective longitudinal study requires ongoing funding beyond the five year limit provided by the *Discovery Projects* scheme.[105]

---

103 The 1994 survey was commissioned by the Human Rights and Equal Opportunity on behalf of the Privacy Commissioner—this was prior to the establishment of the Office of the Privacy Commissioner. In 2001 the OPC also commissioned surveys on business attitudes and government agency attitudes to privacy. These surveys were not replicated in 2004.

104 The 2001 survey included a comparison between results from the 1994 and 2001 surveys: Roy Morgan Research, *Privacy and the Community [prepared for Office of the Federal Privacy Commissioner]* (2001), Attachment B.

105 Funding for projects can be awarded for one to five years. Fellowships are awarded for three to five years, depending upon the type of fellowship: Australian Research Council, *Discovery Projects: Selection Report for Funding Commencing in 2007* (2007) <www.arc.gov.au> at 31 July 2007.

Proposal 59–1 The Australian Government should fund a longitudinal study of the attitudes of Australians, including young Australians, to privacy.

Online social networking

59.109 The ALRC is aware there are concerns about the way in which young people are using social networking sites. Consistent with its approach to online regulation generally,[106] the ALRC is not making a proposal to regulate social networking sites. The ALRC is, however, making a more general proposal in Chapter 60 to establish age verification and parental consent mechanisms to ensure that decisions under the *Privacy Act* regarding the personal information of children and young people aged 14 and under are made by an authorised representative of the child or young person.

59.110 The ALRC notes that, as a result of the activities of the FTC in implementing COPPA in the United States, and a measure of self-regulation in the growing market, many social networking sites are developing standards for their terms of participation which set age limits and encourage parental monitoring and reporting of under-age use. This approach is to be encouraged, but is unlikely to stop curious children and young people from avoiding simple age verification mechanisms.

59.111 In the ALRC's view, the most effective measure that can be taken at present is to educate children, young people, and their teachers and parents, about social networking sites, their dangers and pitfalls, and how to use them safely and appropriately. The need for education in this area is discussed further below.

Photographs and other images

59.112 In concert with community attitudes on the subject, the ALRC is not proposing a blanket ban on the taking of images without consent. This is not seen as a practical or desirable option. The ALRC notes, however, that there is confusion and concern around issues of taking and publishing images in inappropriate circumstances. The ALRC believes that a multifaceted approach is required to alleviate these concerns.

59.113 The criminal law is an important aspect of the regulation of the more severe forms of inappropriate behaviour. Further consideration must be given to what types of behaviour the community wants to label as criminal, but it is clear that merely taking an image without consent should not be considered a criminal act. It is outside the scope of this Inquiry to examine and improve criminal laws to ensure that the full range of inappropriate behaviour relating to the making and using of offensive images is dealt with effectively in criminal offences. This issue should be progressed further by SCAG to ensure uniformity across the jurisdictions.

---

106 See Ch 8.

59.114 The ALRC notes that, under the proposals in this Discussion Paper, the *Privacy Act* will apply to people acting on behalf of a business, including a small business, and thus cover the collection of images for commercial purposes. However, individuals taking and publishing images for personal use are not covered under the Act.

59.115 As indicated above, the ALRC is giving further consideration to the use of take-down notices to remove online content that is considered to be an invasion of privacy. This could be a practical, cost-effective remedy for individuals faced with publication of offensive material, including images, relating to themselves. It would enable individuals to exercise some control over how images of themselves are published when they are taken without consent. As discussed in Chapter 8, however, there are a number of competing arguments against extension of the existing take-down notice scheme.

59.116 From a privacy perspective, it is the preliminary view of the ALRC that the introduction of a statutory cause of action for invasion of privacy is the most effective way to regulate the issue. This will provide a remedy in cases where there is serious harm arising from the invasion of privacy, and also provide a message to the community in general about what constitutes acceptable behaviour. As discussed in Chapter 5, a statutory cause of action will contain appropriate defences, in particular a public interest defence, which will balance the right of privacy with competing rights, such as freedom of expression. Combined with appropriate criminal offences to deal with the most unacceptable actions, a statutory cause of action allows a balanced way forward to allow indivuals to continue to photograph and video friends and family, and to allow the artistic community to use this medium of artistic expression in an acceptable way, while providing some limits on the invasion of personal privacy.

59.117 It is clear, however, that further information about the laws relating to the taking of images is required in the community. In conjunction with proposals for the introduction of a statutory cause of action for invasion of privacy, the ALRC proposes that the OPC should provide information to the public concerning the statutory cause of action. As the publication of images, particularly in the online environment, is an issue of particular concern to the community, such information should cover the issue of images, and include discussion of when publication of an image is likely to be considered an invasion of privacy.

59.118 Similarly, the proposal below to provide further education to children and young people on privacy issues should include consideration of issues around taking and publishing images, particularly in the online environment.

Privacy education for children and young people

59.119 The ALRC has identified a need to inform and educate young people about privacy issues so that they are better equipped to protect their own privacy and respect the privacy of others. This is particularly so for operating in the online environment, but is relevant more generally to interaction with government, organisations and other individuals. This proposal is intended to equip young people with the necessary information and analytical skills to make appropriate decisions about withholding or disclosing personal information.

59.120 The ALRC has given consideration to who should provide the education and the educational materials. Many adults do not understand adequately their privacy rights.[107] Further, although many adults are starting to use social networking sites, they are often less sophisticated about privacy in this environment than their younger counterparts.[108]

59.121 The ALRC proposes that greater awareness of privacy rights, protection of personal information, and respect for the privacy of others, should be incorporated into primary and secondary schools. Privacy issues should arise when teaching about computers and online safety, in various commerce and legal studies areas, and generally in civics and citizenship education. To facilitate privacy education, state and territory education departments should incorporate privacy issues, and in particular privacy in the online environment, into school curricula. Teachers should be able to draw on educational materials proposed in this chapter, as well as existing material available online.

59.122 There are a number of websites which provide information and in some cases software tools to assist with controlling privacy in the online environment.[109] The Australian Communications and Media Authority provides advice and guidance to children, young people and parents on a number of telecommunications issues, such as safe use of mobile chat services and not providing identifiable photographs when using these services.[110] Many of the social networking sites include extensive tips and suggestions for controlling privacy of individual profiles, and have protocols for reporting abusive behaviour. Young people are primarily learning their online social networking skills from peers, however, and peers do not always know or pass on the important safety and privacy awareness tips that need to be learned. For this reason the ALRC considers that an introduction to these issues within the school environment will

---

107 In the 2004 Australian survey of community attitudes to privacy, 35% indicated they had some level of knowledge, 34% indicated very little, and 4% said they had no knowledge of their rights when it comes to protecting personal information—only 22% indicated they had an adequate amount of knowledge, and 4% said they had a lot of knowledge: Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 11.

108 See, eg, D Devlin, *Baby Pics on the Net: Public or Private?* (2007) Yahoo? Tech <tech.yahoo.com/blogs/devlin/11228> at 1 August 2007 and comments posted at that site.

109 See Ch 6 for a full discussion of privacy enhancing tools for the online environment.

110 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

help to equip young people with the necessary skills to identify and manage privacy and safety issues.

59.123 There has already been some recognition of the need to provide specific education about social networking sites to young people. In October 2006, the Information and Privacy Commissioner of Ontario, in conjunction with Facebook, launched a pamplet about selecting and using social networking sites.[111] Aimed at college students, who, until recently, were the primary users of Facebook, the pamphlet addresses some of the key issues to consider when developing profiles and operating in the social networking environment. More recently, the Australian Privacy Commissioner noted concerns about privacy awareness for participants of social networking sites as part of the launch of an international privacy competition for secondary students.[112]

59.124 The ALRC considers there to be a role for the OPC more generally to develop educational material about privacy aimed at children and young people. The Human Rights and Equal Opportunity Commission provides a range of resources on its website for students and teachers to incorporate human rights issues and case studies into lesson plans. The OPC presently has a range of web pages and information sheets aimed at individuals to provide guidance on the operation of the *Privacy Act*. However, the development of material aimed at a younger audience, and geared towards school curricula, would make the information more accessible to children and young people. The ALRC has found this approach useful in developing its *Talking Privacy* website for this Inquiry. The incorporation of OPC materials into student lessons may also help to raise the profile of the OPC among young people, better enabling them to access further information and the complaint handling processes available to them.

59.125 Another body that should be involved in developing educational material covering privacy issues in the online environment is NetAlert, Australia's internet safety advisory body. Established in 1999 by the Australian Government, it is a not-for-profit community organisation that provides advice and education on internet safety issues. In addition to information for parents and teachers, the NetAlert website includes a number of interactive educational programs on internet safety, including: Netty's World aimed at young children to age 7; CyberQuoll aimed at upper primary school students; Cybernetrix aimed at secondary school students; and Wise Up To IT aimed at young people aged 16 and over.[113]

---

111 Information and Privacy Commissioner of Ontario, 'Think About Your Privacy When Selecting a Social Networking Site: Commissioner Cavoukian' (Press Release, 12 October 2006). See also brochure Information and Privacy Commissioner of Ontario and Facebook, *When Online Gets Out of Line—Privacy: Make an Informed Online Choice [pamphlet]* (2006).

112 B Smith, 'Prizes on Offer for Privacy Week', *The Age* (Melbourne), 28 May 2007, 3.

113 All of the sites are linked from NetAlert, *Website* <www.netalert.com.au> at 1 August 2007.

59.126 The educational materials are of high quality, and in an age-appropriate way cover topics such as inappropriate content, cyber bullying, stalking and paedophile activity, computer security, and identity theft. All of the material focuses on the dangers of chat sites, but has not yet addressed the newer realities of social networking sites.[114] CyberQuoll, for example, aimed at younger students, provides a good scenario on the dangers of posting photographs online, and considers the consequences of peer use of the photographs as well as paedophile activity. At present, the older age group Cybernetrix program does not give much information on social networking sites, although it does alert young people to the dangers of providing personal information online and provides links to the OPC website. The Wise Up To IT site has a more limited breadth of material.

59.127 As a body whose educational material is already used extensively in the school and home environment, NetAlert would be ideally placed to develop material about social networking and ensure that the relevant safety and privacy issues are introduced to children and young people. The ALRC proposes that NetAlert update its existing educational material or introduce new material to cover online social networking issues for a range of age groups.

Proposal 59–2 The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.

Proposal 59–3 NetAlert should include specific guidance on using social networking sites as part of its educational material on internet safety.

Proposal 59–4 In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curricula.

114 However, the NetAlert site contains some limited information on social networking sites, including some safety tips: NetAlert, *What Are Social Networking Web Sites?* <www.netalert.com.au/03604-What-are-social-networking-web-sites.asp> at 1 August 2007.

Part I

Children, Young People and Adults Requiring Assistance

60. Decision Making by Individuals Under the Age of 18

Contents

Introduction 1751
Privacy rights of children and young people at international law 1753
Existing Australian laws relating to privacy of individuals under the age of 18 1756
Privacy Act 1756
Other privacy legislation 1758
Assessing the decision-making capacity of children and young people 1759
Child development and brain development research 1759
Health information 1765
Submissions and consultations 1769
Possible models for assessing capacity 1774
ALRC's view 1779
Specific privacy issues affecting children and young people 1787
Online consumers and direct marketing issues 1787
Schools 1795
Child care services 1804
Media 1806
Identification in criminal matters and in court records 1810
Family law 1813
Child welfare and juvenile justice 1814

Introduction

60.1 There is no federal legislation specifically addressing the privacy of children and young people. While the *Privacy Act 1988* (Cth) applies to individuals under the age of 18, there is no provision dealing explicitly with the particular needs of children and young people. It is not always clear how the Act applies to these individuals, or who can and should make decisions about privacy on behalf of an individual under the age of 18.

60.2 The need for the *Privacy Act* to address children's privacy was discussed at the time of passage of the *Privacy Amendment (Private Sector) Act 2000* (Cth). The Opposition moved amendments that would require a 'commercial service' to obtain the consent of a child's parent before collecting, using or disclosing personal information

concerning a child aged 13 or under.[1] While the amendment was not agreed to, the Government indicated that the issue would be investigated further.[2]

60.3 In 2001, the then Attorney-General, the Hon Daryl Williams MP, announced the establishment of a consultative group on children's privacy, convened by the Attorney-General's Department.[3] The consultative group met twice but, despite plans for publication of a discussion paper on children's privacy, the matter has not progressed.[4]

60.4 Children's privacy was exempted specifically from the review of the private sector provisions of the *Privacy Act* that was completed by the Office of the Privacy Commissioner (OPC) in 2005.[5] The 2005 review of the *Privacy Act* by the Senate Legal and Constitutional References Committee did not examine children's privacy and made no recommendations on the issue.[6]

60.5 This chapter considers a number of issues about decision making by and for individuals under the age of 18, and what, if any, changes are needed in the *Privacy Act* or other legislation to clarify these matters. Generally, the ALRC supports the existing approach that individuals under the age of 18 should be assessed individually to determine whether they have the capacity under the Act to make a decision. To support this assessment, the ALRC proposes that the Act be amended to define more clearly the meaning of capacity. The ALRC also proposes a range of mechanisms, including guidance from the OPC and training and education for staff in agencies and organisations, aimed at ensuring that appropriate assessments are undertaken.

60.6 The ALRC has also recognised, however, that there are many situations where individual assessment is not possible, and proposes an age at which an individual is presumed to have capacity to make a decision on his or her own. After considering the latest research on child development and the brain development of adolescents, and community debates about ages of capacity, the ALRC proposes that the age be set at 15. Below this age, it is proposed that an individual who has not been assessed individually should be considered incapable of making a decision under the *Privacy*

---

1 The amendment was headed 'Special protection for children': Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus). The amendment was supported by the Australian Democrats: Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 November 2000, 20162 (N Stott Despoja), 20165.

2 The Government acknowledged that the notion of children's privacy had merit, but that the form of the amendment needed consultation before it could be accepted: Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2000, 20304 (A Vanstone—Minister for Justice and Customs).

3 D Williams (Attorney-General), 'First Meeting of Consultative Group on Children's Privacy' (Press Release, 4 June 2001).

4 Australian Government Attorney-General's Department, *Fact Sheet on Privacy in the Private Sector—Children's Privacy* (2000) <www.ag.gov.au> at 1 August 2007.

5 The terms of reference for that review stated that children's privacy was one of 'certain aspects of the private sector provisions [which] are currently, or have recently substantively been, the subject of separate review': Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 22, App 1.

6 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

Act. The ALRC proposes a number of new provisions for the *Privacy Act* to implement this policy, and to define who is capable of making a decision on behalf of an individual who is not capable of making a decision under the Act.

60.7 The ALRC considered proposing the introduction of additional protections for children and young people under the *Privacy Act*. The primary area of concern was the interaction between direct marketers and children in the online environment. In the ALRC's view, however, the *Privacy Act*, if amended in accordance with the proposals in this Discussion Paper, would operate to provide adequate protection for the personal information of children and young people.

60.8 Other areas considered in this chapter are schools and the media. While the ALRC does not propose any legislative change to address concerns relating to the handling of personal information of students in schools, it is proposed that schools clarify certain issues in their Privacy Policies; in particular, the disclosure of student information to parents, and the responsibilities of school counsellors to disclose information to school management and parents. Consistent with proposals made in Chapter 38 on the media exemption, the ALRC proposes that the privacy of children and young people be given particular consideration when assessing the adequacy of media privacy standards for the purposes of the media exemption.

Privacy rights of children and young people at international law

60.9 Chapter 1 notes the recognition of privacy as a human right in a number of international conventions. The specific right of privacy for children is also set out in art 16 of the United Nations *Convention on the Rights of the Child 1989* (CROC).[7]

> 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
>
> 2. The child has the right to the protection of the law against such interference or attacks.

In addition, art 40(2)(b)(vii) of CROC refers to the specific need to have respect for the privacy of a child accused or found guilty of a criminal offence.

60.10 The articles deal with information privacy, including such things as rights to confidential advice and counselling, and control of access to information stored about the child in records or files. The articles have also been interpreted to cover 'privacy' in terms of physical environment and the privacy of relationships and communications

---

7 *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990). 'Child' is defined in the Convention as a person under the age of 18.

with others.[8] For example, a concern of the United Nations Committee on the Rights of the Child is the personal space provided to, and the regulation of communications of, children and young people in institutional care, including in juvenile justice facilities and immigration detention.[9]

60.11 CROC was adopted by the United Nations in November 1989 and ratified by Australia in December 1990, coming into effect in Australia in January 1991.[10] It is the most universally accepted international convention.[11] Any federal, state or territory legislation, policy or practice that is inconsistent with CROC places Australia in breach of its international obligations, and could have consequences at the international level.[12]

60.12 A number of other international guidelines relating to the rights of children make reference to the need to protect privacy, including the *United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985* (the Beijing Rules)[13] and the *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty 1990*.[14] Although not necessarily binding on Australia at international law, these rules represent internationally accepted minimum standards and are important reference points in developing policy.

60.13 CROC has aroused significant misgivings within some sections of the Australian community, and in other countries, about the interaction between the rights of children and governments and the rights of parents to raise their family in the way

---

8 UNICEF, *Implementation Handbook for the Convention on the Rights of the Child* (fully revised ed, 2002).

9 J Doek—Chairperson UN Committee on the Rights of the Child, *Consultation PM 14*, Sydney, 18 August 2006.

10 While CROC has been ratified by Australia, it has not been fully implemented into Australian domestic legislation. Australia's international law obligations are relevant to the interpretation of Australian statutes, and Australian courts generally will interpret legislation to reach a result that is inconsistent with Australia's international law obligations only if there is 'a clear indication that the legislature has directed its attention to the rights or freedoms in question, and has consciously decided upon abrogation or curtailment': *Plaintiff S157/2002 v Commonwealth* (2003) 211 CLR 476, [30]. For a detailed exposition of the influence of international law (and especially international human rights law) on Australian municipal law, see R Piotrowicz and S Kaye, *Human Rights: International and Australian Law* (2000).

11 Many countries have placed reservations and declarations on a number of articles. Australia has a reservation in relation to art 37(c) based on physical size and population distribution difficulties in ensuring the separation of young offenders and adult offenders while enabling young offenders to maintain contact with their families: Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [20.102].

12 Except in relation to art 37(c).

13 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985). See in particular rule 8, which is discussed below in relation to access to court records.

14 *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty*, UN Doc A/RES/45/113 (1990). See in particular rule 19 on records.

they believe to be most appropriate.[15] These concerns were also present during the drafting of the Convention, and led to the inclusion of art 5, which reads:

> States Parties shall respect the responsibility, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

60.14 CROC embodies a balancing exercise, recognising that the family is the fundamental unit of society, but that children are individuals who are not wholly subsumed by family. The rights set out in CROC are the rights of children which should be respected by their families, communities and governments. Article 5 clearly anticipates that, while a child should be guided appropriately by parents and others in exercising his or her rights, a child will also become more independent of family as his or her capacities develop. It is at this point—where a child becomes a young person with needs and wishes separate from his or her parents—that difficulties may arise in determining whether a child should be able to exercise rights on his or her own behalf. Article 12 of CROC, which refers to a child's right to be heard in matters affecting the child, makes a similar assumption regarding the evolving capacity of children.[16]

60.15 Consistent with CROC, most rights and responsibilities in Australian law refer to a person as an adult when he or she turns 18 years of age.[17] While historically the law has generally assumed that children do not have the capacity to participate in legal processes on their own behalf, more recent psychological studies have provided a greater understanding of children's cognitive abilities and prompted a re-evaluation of rules regarding children's capacity.[18] Increasingly, the common law and particular statutes are recognising the ability of young people at an age lower than 18 to make decisions on their own behalf, even where this may conflict with the wishes of their parents.

---

15 Parliament of Australia—Joint Standing Committee on Treaties, *United Nations Convention on the Rights of the Child* (1998), [1.36]; M Otlowski and B Tsamenyi, 'Parental Authority and the United Nations Convention on the Rights of the Child: Are the Fears Justified?' (1992) 6 *Australian Journal of Family Law* 137.

16 The article requires that 'the child who is capable of forming his or her own views' should have the right to express those views, and that the views should be 'given due weight in accordance with the age and maturity of the child': *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990) art 12(1).

17 This varies, however, particularly in the area of juvenile justice: see L Blackman, *Representing Children and Young People: A Lawyers Practice Guide* (2002), 4–5.

18 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [4.7]–[4.9]; Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [4.4]–[4.9], [14.19]–[14.24]. The research is discussed in more detail below.

Existing Australian laws relating to privacy of individuals under the age of 18

Privacy Act

60.16 The personal information of individuals under the age of 18 is regulated by a number of laws. The laws that apply will depend upon who holds the information, although generally personal information held by Commonwealth and ACT agencies or their contactors, or held by non-government bodies not otherwise exempt from the operation of the Act, is regulated by the *Privacy Act*.[19] Many of the ALRC's proposals to streamline and clarify the operation of the *Privacy Act* and other privacy laws in Australia will also improve the handling of personal information of individuals under the age of 18.[20] In particular, the ALRC proposes that the Information Privacy Principles (IPPs) that apply to agencies, and the National Privacy Principles (NPPs) that apply to organisations, be replaced with a single set of principles, referred to in this paper as the Unified Privacy Principles (UPPs).[21]

60.17 Many aspects of the IPPs and NPPs, and the proposed UPPs, may require an individual to provide consent to the collection, use or disclosure of personal information about him or her. The Act also establishes a number of situations where an individual can make a request or exercise a right. Each of these situations has a decision-making element. These include:

- consenting to the collection of sensitive information;[22]
- consenting to a particular use or disclosure of personal information, including consent to use such information for the purpose of direct marketing;[23]
- consenting to the transfer of personal information outside of Australia;[24]
- requesting not to receive further direct marketing communications from an organisation;[25]
- requesting access to personal information held by an organisation;[26]

---

19 For a more detailed analysis of the scope of existing privacy laws in Australia, see Ch 2.

20 These proposals include harmonisation of information privacy laws across jurisdictions (Proposals 4–1, 4–2, 4–3, 4–4, 4–5), amendment of the Act to achieve greater logical consistency, simplicity and clarity (Proposal 3–2), and inclusion of an objects clause in the Act (Proposal 3–4).

21 See Proposal 15–2.

22 See proposed 'Collection' principle and discussion in Ch 18.

23 See proposed 'Use and Disclosure' principle and 'Direct Marketing' principle and discussion in Chs 22 and 23.

24 See proposed 'Transborder Data Flows' principle and discussion in Ch 28.

25 See proposed 'Direct Marketing' principle and discussion in Ch 23.

26 See proposed 'Access and Correction' principle and discussion in Ch 26. It is proposed that access to personal information held by an agency should be governed by a separate Part of the *Privacy Act*.

- opting for anonymity or pseudonymity in transacting with an agency or organisation;[27] and

- making a complaint against an agency or organisation.[28]

60.18 A number of other requirements set out in the proposed UPPs aim to provide information to the individual to alert him or her to the circumstances of the collection, use and disclosure of personal information about him or her.[29] In some cases, this information will assist an individual in deciding whether to provide or withhold consent to a particular collection, use or disclosure, or to make a request under the Act.

60.19 The *Privacy Act* sets no minimum age at which an individual can make decisions regarding his or her own personal information. Guidelines developed by the OPC provide some assistance in dealing with children and young people. The *Guidelines to the National Privacy Principles* suggest that each case must be considered individually, and give guidance as to when a young person may have the capacity to make a decision on his or her own behalf.

> As a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity of understanding to do so themselves.[30]

60.20 The *Guidelines on Privacy in the Public Health Sector* stress that where a young person is capable of making his or her own decisions regarding personal information, he or she should be allowed to do so.[31] The Guidelines further suggest that, even if the young person is not competent to make a decision, his or her views should still be considered.[32]

---

27 See proposed 'Anonymity and Pseudonymity' principle and discussion in Ch 17.

28 See discussion in Ch 45.

29 See, eg, proposed 'Specific Notification' principle, which requires an agency or organisation to take reasonable steps to ensure the individual is aware of a list of factors relating to the collection and use of their personal information, and proposed 'Openness' principle, which requires agencies and organisations to create a Privacy Policy: Chs 20, 21.

30 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 21. Guidelines relating to the IPPs are more ambivalent, noting it may not be appropriate to rely on consent given by another person if a person under the age of 18 years is sufficiently old and mature to consent on their own behalf: Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11: Advice to Agencies about Using and Disclosing Personal Information* (1996), 29.

31 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 33.

32 Ibid, 34.

60.21 At present, only one of the NPPs and IPPs, and no other provision of the *Privacy Act*, sets up a structure for making decisions on behalf of an individual unable to make a decision concerning the privacy of his or her personal information. This structure relates to disclosure of health information in limited circumstances.[33] It is assumed that parents are responsible for making decisions on behalf of children or young people incapable of making the decision themselves.[34]

Other privacy legislation

60.22 Some states and territories have legislation or administrative practices that regulate the privacy of certain personal information held by state or territory public sector agencies.[35] Most apply specifically to health information and these are discussed in more detail in Chapter 2.

60.23 Generally, these statutes and schemes adopt the same approach to children and young people as the *Privacy Act* in that individuals under the age of 18 are given the same rights and protections as adults, and there are no specific protections or additional provisions relating to children or young people.

60.24 Unlike the *Privacy Act*, however, some of the legislation provides statutory guidance regarding when a child or young person will be considered capable of making decisions without a parent or guardian regarding his or her own personal information. For example, s 85(3) of the *Health Records Act 2001* (Vic) states:

> (3) For the purposes of sub-sections (1) and (2), an individual is incapable of giving consent, making the request or exercising the right of access if he or she is incapable by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of—
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or
>
> (b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires)—
>
> despite the provision of reasonable assistance by another person.[36]

---

33 NPP 2.4 allows disclosure of health information to a 'responsible' third party in the event that an individual is incapable of giving or communicating consent for disclosure, and the disclosure is necessary for the care or treatment of the individual or for compassionate reasons: *Privacy Act 1988* (Cth) sch 3, NPP 2.4. A 'responsible' person is defined to include a parent of the individual: *Privacy Act 1988* (Cth) sch 3, NPP 2.5.

34 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 213.

35 For an overview of privacy regulation in the states and territories, see Ch 2.

36 If the child is incapable, the giving, making or exercising of the consent, request or right may be provided by a parent or other authorised representative of the child: *Health Records Act 2001* (Vic) s 85(6). Part 4 cl 4(3) of the draft *National Health Information Code* is an identical provision, and the *Health Records and Information Privacy Act 2002* (NSW) s 7 has a similar operation.

60.25 In the *Health Records (Privacy and Access) Act 1997* (ACT), the test of capacity is linked to the ability to understand the nature of, and give consent to, a health service.[37] Some legislation also includes express provisions on how, and by whom, decisions can be made on behalf of a child or young person unable to make his or her own decisions.

Assessing the decision-making capacity of children and young people

Child development and brain development research

60.26 There is clear evidence that children differ from adults in their capacity to make decisions.[38] It is not clear, however, at what age an individual should be regarded as having the capacity to make a decision regarding his or her own personal information. The following provides an overview of the research on the issue.

Ages of development

60.27 There is a general consensus in the literature on child development that the capacity of children to make voluntary and rational decisions increases with both age and the development of cognitive skills.[39] Decision making is a skill that develops over time together with the development of certain cognitive skills, including the capacity for logical thought, the ability to understand cause and effect, and the analysis of consequences of decisions. Jean Piaget, a leading child psychologist, identified four stages of cognitive development through which all children pass and the typical ages at which this development occurs.[40] It is during the fourth stage—the 'formal operations' period—that a child demonstrates adult-like thinking abilities such as a comprehension of abstract logic, a capacity to reason, the use of deductive and inductive reasoning, making of intelligent choices, and the ability to hypothesise. According to Piaget, a child aged between 11 and 15 is generally in this stage.

60.28 Piaget's typology, including the allocation of typical ages at which certain developments occur, resonates with research about the decision-making capacities of

37 'Young person' is defined as a person under 18 years of age other than a person 'who is of sufficient age, and of sufficient mental and emotional maturity, to (a) understand the nature of a health service; and (b) give consent to a health service', and the rights of a young person are to be exercised by a parent or guardian: *Health Records (Privacy and Access) Act 1997* (ACT) s 25, Dictionary.

38 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 349.

39 Ibid, 348. A child's competency, however, may not necessarily increase in direct relation to his or her age: S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 315.

40 D Singer and T Revenson, *A Piaget Primer: How A Child Thinks* (revised ed, 1996), 20–26.

children.[41] In her examination of the literature on the capacity of minors to provide voluntary consent to medical treatment, Dr Tara Kuther notes:

> During the adolescent years, minors become better able to consider information and opinions from diverse sources, and capable of owning their judgements. Between the ages of 15 and 17, most adolescents become capable of providing voluntary consent that is not unduly influenced by others.[42]

60.29 Kuther also discusses the way in which children exercise more independence in making decisions as they become older. In particular she notes:

> Young children tend to view authority figures such as physicians and parents as legitimate and powerful, and are likely to comply with their requests because of differences in perceived social power. With increasing age, authority figures tend to be viewed as cooperative and orientated toward promoting social welfare; adolescents are more likely to question demands that seem unreasonable and are less susceptible to coercive influence.[43]

60.30 Many commentators argue that young people that have reached a certain age have the same capacity as adults to consent to decisions. The area that has received the most attention is the capacity of an individual to consent to medical treatment. In a study comparing the competency of individuals aged 9, 14, 18 and 21 to make informed decisions about medical treatment, Drs Lois Weithorn and Susan Campbell found that, in general, 14 year olds demonstrated the same level of competence as those aged 18 years and over.[44] The researchers used four standards of competency to test the making of hypothetical medical decisions: (1) evidence of choice; (2) reasonable outcome; (3) rational reasons; and (4) understanding.[45] Weithorn and Campbell noted that while 9 year olds were less competent to make a rational decision, even they were able to comprehend the basics of what is required of them when they are asked to give a preference for treatment.[46]

---

41 S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 312–313.

42 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 348, citing C Lewis, 'Minors' Competence to Consent to Abortion' (1987) 42 *American Psychologist* 84 and T Grisso and L Vierling, 'Minors' Consent to Treatment: A Developmental Perspective' (1978) *Professional Psychology* 412.

43 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 347, citing W Damon, 'Measurement and Social Development' (1977) 6(4) *Counselling Psychologist* 13 and R Thompson, 'Vulnerability in Research: A Developmental Perspective on Research Risk' (1990) 61 *Child Development* 1.

44 L Weithorn and S Campbell, 'The Competency of Children and Adolscents to Make Informed Treatment Decisions' (1982) 53 *Child Development* 1589.

45 The four hypothetical dilemmas were diabetes, epilepsy, depression and enuresis.

46 Weithorn and Campbell cautioned, however, that their findings are limited in so far as their subjects were 'normal, white, healthy individuals of higher intelligence and middle-class background and that the situations they considered were hypothetical': L Weithorn and S Campbell, 'The Competency of Children and Adolscents to Make Informed Treatment Decisions' (1982) 53 *Child Development* 1589, 1596.

60.31 Based on her research, Kuther suggests that young people aged 15 can make decisions concerning medical treatment.[47] Sarah Ramsey suggests somewhere between 14 and 16.[48]

60.32 Although the evidence suggests that decision-making abilities are linked to age, the evidence also suggests that it is not possible to identify an age above which *all* children are competent to make decisions and below which *all* children are not competent.

Brain development and psychosocial factors

60.33 In addition to the more traditional child development research, there is a growing body of research into the brain development of adolescents and the relationship between brain development and the capacity of adolescents to make decisions. This research does not necessarily contradict the earlier research on the stages of child development, but adds an additional element to an understanding of the process and outcomes of decision making by adolescents.

60.34 The frontal lobe of the brain is responsible for functions such as organising thoughts, setting priorities, planning and making judgments. Scientists have discovered that the frontal lobe of the brain undergoes significant change during adolescence, in which it produces a significant amount of 'grey matter' (the brain tissue responsible for thinking) and then undergoes a period in which it rapidly thins or 'prunes' the grey matter and develops 'white matter' (the brain tissue responsible for making the brain operate precisely and efficiently).[49] The research suggests that the frontal lobe, and therefore an individual's decision-making capacity, has not reached full maturity until some time in a person's early twenties.[50]

60.35 Other research looking at how different parts of the brain interrelate has led researchers to conclude that adolescents rely more heavily than adults on the parts of the brain that react to emotion than on the more logical frontal lobe, possibly because

---

47 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 350.

48 S Ramsey, 'Representation of the Child in Protection Proceedings: The Determination of Decision-Making Capacity' (1983–1984) 17 *Family Law Quarterly* 287, 314.

49 C Wallis and K Dell, 'What Makes Teens Tick', *Time Magazine* (online), 10 May 2004, <www.time.com>; J Fagan, 'Adolescents, Maturity, and the Law', *The American Prospect* (online), 14 August 2005, <www.prospect.org>; A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2, citing E Sowell et al, 'In Vivo Evidence for Post-Adolescent Brain Maturation in Frontal and Striatal Regions' (1999) 2 *Nature Neuroscience* 10 and E Sowell et al, 'Mapping continued Brain Growth and Gray Matter Density Reduction in Dorsal Frontal Cortex: Inverse Relationships During Post-Adolescent Brain Maturation' (2001) 21 *Journal of Neuroscience* 22.

50 A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2. See also L Bowman, *New Research Shows Stark Differences in Teen Brains* (2004) Death Penalty Information Center <www.deathpenaltyinfo.org> at 1 August 2007, 1.

the frontal lobe is still maturing.[51] As a result, it has been suggested that adolescents allow their emotional responses to situations to determine their course of action and do not fully evaluate the consequences of a particular course of action before commencing it.[52] One study has shown that age differences in decision making and judgment become most apparent when the decisions of adolescents in emotionally charged or highly social situations are compared with the decisions of adults in similar situations. For example, it has been found that adolescents take more risks when in the presence of their peers than do adults.[53]

60.36 While some have cautioned against jumping to conclusions about adolescent decision-making capacity based on the latest brain research,[54] the findings and suggestions are consistent with a review of the studies by Elizabeth Cauffman and Professor Laurence Steinberg on the susceptibility of adolescents to influence. Cauffman and Steinberg identify three themes that emerge from research on age difference in decision-making priorities:

- in comparison to adults, adolescents view long-term consequences as less important than short-term consequences;
- 'sensation seeking' is a higher priority for adolescents than it is for adults; and
- social status among peers is an important factor for many adolescents.[55]

60.37 Cauffman and Steinberg argue that the big difference between decision making by individuals under the age of 18 and adults is that psychosocial factors can influence the use of cognitive skills by young people during the decision-making process.[56] Three components make up these psychosocial factors:

- *responsibility*, including health autonomy, clarity of identity and self-reliance;
- *perspective*, which is the 'ability to acknowledge the complexity of a situation and see it as part of a broader context'; and

---

51 D Yurgelun-Todd, *Inside the Teenage Brain: Interview* (2002) Public Broadcasting Services <www.pbs.org/wgbh/pages/frontline/shows/teenbrain/interviews/todd.html> at 1 August 2007.

52 A Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center—American Bar Association, 2; J Fagan, 'Adolescents, Maturity, and the Law', *The American Prospect* (online), 14 August 2005, <www.prospect.org>.

53 C Wallis and K Dell, 'What Makes Teens Tick', *Time Magazine* (online), 10 May 2004, <www.time.com>, 6.

54 *Inside the Teenage Brain: Introduction* (2002) Public Broadcasting Service <www.pbs.org/wgbh/pages/frontline/shows/teenbrain/etc/synopsis.html> at 1 August 2007.

55 E Cauffman and L Steinberg, 'The Cognitive and Affective Influences on Adolescent Decision-Making' (1995) 68 *Temple Law Review* 1763, 1772–1773.

56 Ibid, 1770.

- *temperance*, which is the 'ability to limit impulsive and emotional decision making, to evaluate situations thoroughly before acting … and to avoid decision-making extremes'.[57]

60.38 This is not to suggest that adolescents are unable to make decisions on their own. The results of the research are consistent, however, with the approach that stresses that an individual's capacity to make a decision cannot be determined by age alone: it also depends on the maturity of the individual, his or her social development, including his or her relational style with authority and cultural and religious background,[58] and sense of self.[59] Importantly, an individual's capacity to make a decision also depends on the particular decision that needs to be made, its complexity and the gravity of the consequences.[60] This makes an adolescent's maturity of judgment for making a decision highly situation-specific.[61] In the context of making medical decisions, Assistant Professor Leanne Bunney has noted:

> merely because a child may not have the capacity to make decisions in one area does not necessarily imply that he or she would be unable to make decisions in relation to other treatment.[62]

Evolving capacity and the need for individual assessment

60.39 The research suggests, therefore, that the capacity of a child or young person to make a decision is evolving and dependent on a number of considerations relevant to the individual and the particular decision. As discussed above, this understanding of capacity is reflected in art 5 of CROC.

60.40 An individual approach to assessing the capacity of a child or young person has been adopted in case law. The House of Lords decision in *Gillick v West Norfolk and Wisbech AHA* (*Gillick*), and the High Court of Australia decision in *Department of Health and Community Services (NT) v JWB* ('*Re Marion*'), reflect the concept of evolving capacities and the need for individual assessment.[63] In *Re Marion*, Deane J stated that:

---

57 Ibid, 1764.

58 M McCabe, 'Involving Children and Adolscents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Pediatric Psychology* 505.

59 L Weiss Roberts, 'Informed Consent and the Capacity for Voluntarism' (2002) 159 *American Journal of Psychiatry* 705.

60 R Ludbrook, 'Children and the Political Process' (1996) 2 *Australian Journal of Human Rights* 278, 376; P Tuohy, 'Children's Consent to Medical Treatment' (2001) *New Zealand Law Journal* 253.

61 E Cauffman and L Steinberg, 'The Cognitive and Affective Influences on Adolescent Decision-Making' (1995) 68 *Temple Law Review* 1763, 1775.

62 L Bunney, 'The Capacity of Competent Minors to Consent to and Refuse Medical Treatment' (1997) 5 *Journal of Law and Medicine* 52, 56.

63 *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112; *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218.

> the legal capacity of a young person to make decisions for herself or himself is not susceptible of precise abstract definition. Pending the attainment of full adulthood, legal capacity varies according to the gravity of the particular matter and the maturity and understanding of the particular young person.[64]

60.41 The words of Deane J, and the individual approach to assessing capacity of a minor, were adopted by the Full Court of the Family Court of Australia in *B and B v Minister for Immigration and Multicultural and Indigenous Affairs*, which considered the capacity of a minor voluntarily to terminate migration detention.[65] Unlike the *Gillick* approach, however, which requires a positive inquiry as to the capacity of a minor to make a particular decision, it has been argued that the Court's approach in *B and B* suggests that capacity is presupposed in some matters, although may be found to be lacking due to certain factors.[66] The Court listed a number of factors, which, in its opinion, may affect the competence of a child, including 'isolation, English language skills, schooling, access to resources and administrative barriers'.[67] Age was considered to be just one factor to take into consideration. This approach has not as yet been followed in other cases.

Assisting children and young people to make decisions

60.42 In addition to developing decision-making abilities with age, children also develop the capacity to make decisions by being involved in decision-making processes.[68] Dr Mary Ann McCabe argues that 'children's preferences and capacity for involvement in medical decision making will be heavily influenced by their prior experience with taking responsibility in decisions'.[69] McCabe suggests that such experience includes children making different types of decisions in their everyday lives, such as the time they will go to bed.[70]

60.43 Some researchers argue that children have the ability to comprehend difficult concepts that are important for making decisions when the concepts are presented to

---

64 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218, 293.

65 *B and B v Minister for Immigration and Multicultural and Indigenous Affairs* (2003) 199 ALR 604, [373]. The children involved in the case were aged 5, 9, 11, 12 and 14, and were detained with their parents who were appealing refusal of their claim for refugee status.

66 J Morss, 'But for the Barriers: Significant Extensions to Children's Capacity' (2004) 11 *Psychiatry, Psychology and Law* 319, 319. The High Court of Australia overturned the Full Court of the Family Court's decision concerning its jurisdiction over the welfare of children detained under the *Migration Act 1948* (Cth); however the Full Court of the Family Court's discussion of capacity was not considered by the High Court: see *Minister for Immigration and Multicultural and Indigenous Affairs v B and B* (2003) 219 CLR 365.

67 *B and B v Minister for Immigration and Multicultural and Indigenous Affairs* (2003) 199 ALR 604, [379].

68 M McCabe, 'Involving Children and Adolscents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Pediatric Psychology* 505 and R Ludbrook, 'Children and the Political Process' (1996) 2 *Australian Journal of Human Rights* 278.

69 M McCabe, 'Involving Children and Adolscents in Medical Decision Making: Developmental and Clinical Consideration' (1996) 21 *Journal of Pediatric Psychology* 505, 510.

70 Ibid, 510.

them in ways that are 'developmentally appropriate'.[71] Nigel Thomas and Claire O'Kane argue that, unless the views of children are sought in ways that enable them to use their competence, children may erroneously be considered incompetent.[72]

Health information

60.44 The provision of health services to, and the handling of health information about, children and young people is an area that has received more attention than others when considering the decision-making capacity of individuals under the age of 18.

60.45 Consent to the handling of health information about children and young people is related to, but different from, the issue of consent to medical treatment by or on behalf of a child or young person. Although some statutory provisions deal with consent to medical treatment,[73] until the late 20th century the common law assumed that a person under 18 years of age did not have the capacity to make a decision to consent to medical treatment on his or her own behalf. This position has changed. The pivotal case in this area is *Gillick*,[74] which was followed by the High Court of Australia in *Re Marion*.[75]

60.46 These cases affirmed the capacity of 'mature minors' to make their own decisions about medical treatment without parental involvement and reflect the concept of evolving capacities, which is evident in CROC.[76] Neither *Gillick* nor *Re Marion*, however, cover what should be done when a child or young person is assessed as not having capacity to consent to medical treatment, but asks that his or her health information not be disclosed to a parent.[77]

---

71 T Kuther, 'Medical Decision-Making and Minors: Issues of Consent and Assent' (2003) 38 *Adolescence* 343, 347; N Thomas and C O'Kane, 'Discovering What Children Think: Connections Between Research and Practice' (2000) 30 *British Journal of Social Work* 819.

72 N Thomas and C O'Kane, 'Discovering What Children Think: Connections Between Research and Practice' (2000) 30 *British Journal of Social Work* 819, 831.

73 See *Minors (Property and Contracts) Act 1970* (NSW) s 49(2), which covers persons aged 14 years and above; *Consent to Medical and Dental Procedures Act 1985* (SA) s 6(1), which covers persons aged 16 years and above. See also New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004).

74 *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112. This case addressed the issue of whether a minor under the age of 16 years could give consent to contraceptive treatment without the parents' knowledge or consent.

75 *Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218. This case involved an application before the Family Court of Australia for the sterilisation of an intellectually disabled minor, and addressed the issue of limitations on a parent's right to consent to such treatment. For a discussion of the two cases, see P Parkinson, 'Children's Rights and Doctors' Immunities: The Implications of the High Court's Decision in Re Marion' (1992) 6 *Australian Journal of Family Law* 101.

76 See also United Nations Committee on the Rights of the Child, *General Comment No 4: Adolescent Health and Development in the Context of the Convention of the Rights of the Child* (2003).

77 J Loughrey, 'Medical Information, Confidentiality and a Child's Right to Privacy' (2003) 23 *Legal Studies* 510, 512.

60.47 The ability of young people to keep information from their parents and others is often an important consideration when deciding whether to seek medical treatment. This issue is often discussed as 'confidentiality', but the *Privacy Act* and relevant state and territory health information legislation also regulate the disclosure of health information.

60.48 Young people experience a number of barriers in accessing health services, and lack of confidentiality (or a perceived lack of confidentiality) has been identified as a key problem.[78] A US study of high school students indicated that a majority of adolescents have health concerns they wish to keep confidential from their parents, and 25% reported that they would not seek health services because of confidentiality concerns.[79]

60.49 When a doctor sees a patient who is a young person without the attendance of a parent or guardian, the doctor must also assess the young person's capacity to provide consent to the recommended medical treatment.[80] Factors that will be considered by the doctor include the maturity of the young person; the capacity to understand and appreciate the proposed procedure and the consequences of the treatment (as well as possible consequences of not receiving treatment); the gravity of the presenting illness and treatment; and family issues.[81] In most cases involving sensitive or serious health concerns, it is suggested that parental involvement be encouraged, and in many cases the involvement of supportive parents may be a key element of successful treatment.[82] It is not always possible or desirable, however, to involve a parent or guardian in this way.

60.50 Similar factors must be taken into consideration by a doctor when deciding whether information can be disclosed to a parent without the consent of the child or young person. The Australian Medical Association (AMA) has taken the position that

---

78 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004, 21. See also Australian Medical Association, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 22 February 2005, 14; M Booth and others, 'Access to Health Care Among Australian Adolescents: Young People's Perspectives and Their Sociodemographic Distribution' (2004) 34 *Journal of Adolescent Health* 97, 101–103.

79 T Cheng and others, 'Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes Among High School Students' (1993) 269 *Journal of the American Medical Association* 1404.

80 Guidance exists for doctors in dealing with young patients and confidentiality issues. See Medical Practitioners Board of Victoria, *Consent for Treatment of Confidentiality in Young People* (2004); Osteopaths Registration Board of Victoria, *Consent for Treatment of Confidentiality in Young People* (2005); New South Wales Association for Adolescent Health, *Working with Young People: Ethical and Legal Responsibilities for Health Workers* (2005). The National Youth Divisions has an online training course on adolescent health, which includes discussion on confidentiality and capacity to consent to treatment: National Divisions Youth Alliance, *GP Online Training Course* (2006) <ndya.adgp.com.au> at 23 August 2006.

81 L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410, 411. Family issues may include cultural issues, and also where a parent is unable to act in a protective manner (eg, because of substance abuse or severe mental illness).

82 T Stutt and L Nicholls, *Submission PR 40,* 11 July 2006.

if a young person is able to make autonomous decisions regarding medical treatment and wishes the treatment to remain confidential, his or her doctor must respect and maintain that confidentiality.[83] There will, of course, be situations in which the doctor is required to disclose information. Even for adults, there are ethical, statutory and common law exceptions to the duty of confidentiality that require disclosure of information in certain circumstances.[84] Outside of these exceptions, some have argued that confidentiality should be maintained for any young person seeking treatment even if assessed to be incapable of consenting to the appropriate treatment.[85]

60.51 The issue of disclosure of health information to parents sparked public debate in 2003 when the Health Insurance Commission[86] changed its privacy policy to require young people aged 14 and over to give consent before their parents can access their Medicare records.[87] Medicare records include health information such as the identity and speciality of the health service provider, the type of service received, and may also reveal that the individual suffers from certain conditions such as asthma, diabetes, or mental health conditions.[88] The Medicare policy on access to records of an individual under 18 states that:[89]

- if a child or young person of any age has his or her own Medicare card, no information related to the use of the card can be released to a parent or guardian without the consent of the child;[90]

---

83 Australian Medical Association, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 21 December 2004, 21. See also Australian Medical Association, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 22 February 2005, 15.

84 For example, emergency situations with risk of death or serious injury, reporting of certain infectious diseases, or reporting of risk of harm to a child: L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410, 412. For a discussion of disclosure of confidential information in court, see Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 15.

85 See, eg, New South Wales Commission for Children and Young People, *Submission to the New South Wales Law Reform Commission on the Review of Laws Relating to the Consent of Minors to Medical Treatment*, 15 August 2003. See also J Loughrey, 'Medical Information, Confidentiality and a Child's Right to Privacy' (2003) 23 *Legal Studies* 510, 524–525.

86 Now known as Medicare Australia.

87 This policy change, which raised the age from 12 to 14, was based on legal advice: L Sanci and others, 'Confidential Health Care for Adolescents: Reconciling Clinical Evidence with Family Values' (2005) 183 *Medical Journal of Australia* 410. Legal advice to the Australian Government indicated that any further increase of the age would require legislative amendment: T Abbott (Minister for Health and Ageing), 'Parents' Access to Their Children's Medicare Records' (Press Release, 13 November 2003).

88 ABC Radio 891 Adelaide, 'Children's Access to Medicare Cards: Interview with AMA Vice President Dr Mukesh Haikerwal', *Drive with Kevin Naughton*, 6 November 2003.

89 The policy is set out on the Medicare Australia form 'Request for Obtaining Medicare and/or PBS Claims History for a Child'.

90 A young person aged 15 and over can apply for a separate Medicare card without parental approval. A child or young person under the age of 15 can apply for a separate Medicare card with parental approval.

- for a young person aged 14 or 15 on his or her parent's Medicare card, information will not generally be released without the young person's consent, but a parent or guardian may request Medicare Australia to approach any treating medical practitioner to determine if the practitioner will disclose to the parent or legal guardian any information they hold about the young person's treatment; and

- disclosure of information relating to a young person aged 16 and over on his or her parent's Medicare card will only be made available to a parent or legal guardian with the young person's consent.[91]

60.52 Following publication of the changed privacy policy on Medicare records, public debate was split between support for young people's privacy and those concerned that parental rights and family values were being abandoned.[92] The Australian Government announced its intention to introduce the Health Legislation Amendment (Parental Access to Information) Bill to raise the age to 16 and over.[93] Following staunch opposition from certain backbenchers, the AMA and others, however, introduction of the Bill was deferred.[94] It has not since been introduced.

60.53 Discussion on the issue has surfaced more recently in conjunction with the Australian Government's proposed Health and Social Services Access Card. The exposure draft of the Human Services (Enhanced Service Delivery) Bill 2007 (Cth) specifies that an individual under the age of 18 is not entitled to an access card, leading some commentators to express concerns about young people's access to medical benefits and services. Supporting literature issued by the Office of the Access Card notes that, consistent with existing practices, people aged between 15 and 18 years of age will be able to be issued with their own access card without seeking parental

---

91 There are limited exceptions to the non-disclosure principle where a young person is under the age of 18 and on the same card as the requesting parent, including access to a Medicare Financial Taxation Statement which shows a total benefit paid for the year but no details of medical services provided, and access to information about the progress of a Medicare claim made by the parent on behalf of the young person.

92 See, eg, Catholic Health Australia, 'CHA Calls for an Informed Public Discussion, Not Political Point Scoring Over Parental Access to Teenagers' Medical Visits' (Press Release, 10 June 2004). The AMA position is that a person aged 15 or over should have the right to keep his or her Medicare records confidential, as at that age people are making independent decisions about their lives, with some leaving school and entering the workforce. The AMA addressed this as a key health issue in the 2004 federal election: Australian Medical Association, 'Youth Health—The Forgotten Area of Health Policy' (Press Release, 9 September 2004); ABC Radio 666 2CN, 'Medicare Under 16 Legislation: Interview with AMA President Dr Bill Glasson', *Morning with Louise Maher*, 15 June 2004.

93 The announcement included funding in the 2004–05 Budget for implementation of the Bill: Australian Government Department of Health and Ageing, *Budget 2004–2005 Health Fact Sheet 5: A Health System Evolving Through Technology* (2004). See also AAP, 'Abbott Backflips on Teen Medical Records', *Sydney Morning Herald* (online), 15 June 2004, <www.smh.com.au>.

94 T Abbott (Minister for Health and Ageing), 'Parental Access Bill' (Press Release, 15 June 2004); P Hudson, 'Backbencher Fears for Teen Lives', *The Age* (online), 13 June 2004, <www.theage.com.au>; D Wroe, 'Abbott Pulls Teen-Health Records Bill', *The Age* (online), 16 June 2004, <www.theage .com.au>.

permission.[95] It is assumed that individuals aged 15 and over will be given a class exemption as provided for in the Bill.[96]

60.54 The *Privacy Act* and other Australian health information laws reflect the approach taken in medical practice and do not prescribe an age at which a young person is assumed to have, or not have, the capacity to make decisions on his or her own behalf regarding their personal information.[97] The NPPs dealing with sensitive information (which includes health information) require the capacity of a young person to make decisions relating to disclosure of his or her health information to be assessed on a case-by-case basis.[98] This may not be possible where there is not a one-on-one personal relationship between the information holder and the individual, and this is reflected in Medicare Australia's age-based policy for disclosure of records of young people.

Submissions and consultations

Reference to children and young people in the Privacy Act

60.55 Some stakeholders indicated they were comfortable with the absence of a specific reference to children and young people in the *Privacy Act*, although considered that detailed guidance was required to clarify the Act's application to individuals under the age of 18.[99] There was, however, support for specific provisions in the Act covering children and young people.[100] The Queensland Commission for Children and Young People and Child Guardian suggested that it was necessary to recognise in legislation that children and young people have a right to privacy that is separate from the rights of their parents.[101]

60.56 The New South Wales Council for Civil Liberties considered that a separate set of privacy principles applicable to individuals under the age of 18 was necessary due to the unique issues involved.[102] The Legal Aid Commission of New South Wales provided cautious support for the introduction of special provisions for children, so

---

95 Australian Government Office of Access Card, *Fact Sheet—People Under 18 Years of Age* <www.accesscard.gov.au> at 1 August 2007.

96 Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 191. Class exemptions are to be issued by the Minister as a legislative instrument, and subject to disallowance by either House of Parliament. The Bill also provides for exemptions for specified individuals, to be issued by the Secretary as an administrative rule subject to parliamentary scrutiny, but not disallowance: cl 192.

97 The *Privacy Act 1993* (NZ), *Health Information Privacy Code 1994* (NZ) and *Data Protection Act 1998* (UK) also operate in this way.

98 See also Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001).

99 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

100 K Pospisek, *Submission PR 104,* 15 January 2007.

101 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

102 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

long as they did not weaken the principle of equal privacy rights for all.[103] On the other hand, Telstra was opposed to the creation of different rights and obligations for children, as this, arguably, leads to further fragmentation and adds to the regulatory burden on businesses and the community.[104]

Balancing rights of children and young people and parents

60.57 A number of submissions touched on the issue of balancing the rights of children and young people with the rights of parents. The Youth Affairs Council of Victoria (YACVic) noted that the recognition of the evolving capacity of a child is set out in art 5 of CROC, but indicated that an education strategy and appropriate guidelines are required to address the 'grey' areas where it is not clear whether capacity exists.[105] The New South Wales Commissioner for Children and Young People also emphasised that children and young people do not necessarily exclude parents from decision-making processes even as they increase their own involvement.

> Many children and young people tell the Commission that they want their parents to be involved in their lives and to assist them when needed and so want to share their personal information with their parents. However, as young people grow older and seek assistance with more intimate issues they want to choose if and when their parents are involved. Therefore, laws on how information is collected and disclosed need to reflect this need for flexibility.[106]

60.58 One individual suggested that parents should not always be seen as 'baddies' from whom young people need to be protected.[107] It was also noted, however, that the right to access health information of their own child cannot be afforded blindly to all parents. The New South Wales Council for Civil Liberties suggested that there is no automatic right of parents to know about the medical or educational problems of their children, and that the age of the child and the nature of the problem need to be considered.[108] The Caroline Chisholm Centre for Health Ethics also noted the varying quality of child and parent relationships.

> In familial settings there are wide ranging situations where it could be argued that the parent abdicates certain rights that accompany parental responsibility because of neglect, emotional, psychological and physical abuse, or their own drug use, or other harmful behaviour which negatively impacts on the child … It is therefore not possible to argue that it is always in the child's best interest for the parent to be able to access the health information of the child, where the child has independently sought

---

103 Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.
104 Telstra, *Submission PR 185,* 9 February 2007.
105 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007. See also National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.
106 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
107 A Hugo, *Submission PR 285,* 19 April 2007.
108 New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

medical, welfare or social services care, and because of fear or parental reaction, has decided to conceal this information from the parental figure(s).[109]

Capacity of children and young people to make their own decisions

60.59 The existing mechanism in the *Privacy Act*, which does not set an age limit for determining the capacity of an individual under the age of 18, was supported in submissions.[110] The flexible, individual assessment approach was seen as consistent with a rights-based approach to privacy, ensuring the individuality, differing maturity levels and best interests of each child or young person are recognised and considered.[111] The Queensland Commission for Children and Young People and Child Guardian suggested a clear process for making the assessment, which included an onus on the practitioner carefully to explain the consequences of the proposed collection, use or disclosure of the personal information.[112]

60.60 In order for an individual assessment process to work effectively, it was noted that there is a need to provide education to ensure that those making the assessment have the appropriate skills.[113] Consistent with CROC, it was also suggested that children and young people should be involved in decision making, and their views considered, even where the child or young person is considered incapable of making the decision alone.[114]

60.61 There were some who recognised that it is not always possible to make an individual assessment. It was suggested in one submission that unless an assessment can be made about a child's capacity, an agency should refrain from dealing with personal information concerning that child or young person unless legislative provisions permit or require it to do so, or it is otherwise in the best interests of the child.[115] A number of others considered it appropriate to consider setting a specific age

---

109 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006. See also L Mitchell, *Submission PR 46,* 2 June 2006, in relation to children and young people living apart from parents because of a conflict.

110 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007; New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007; Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Australian Retailers Association, *Submission PR 131,* 18 January 2007.

111 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007. See also New South Wales Council for Civil Liberties Inc, *Submission PR 156,* 31 January 2007.

112 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

113 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007; Youth Issues Roundtable, *Consultation*, Melbourne, 7 February 2007.

114 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

115 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

at which an individual is deemed to be capable of making decisions regarding his or her own personal information.[116] Setting an age would ensure consistency of application across the various jurisdictions and the media involving interaction with children and young people.[117] The Australian Health Insurance Association noted that an individual assessment is not realistic in the health insurance setting, and that there is a need to set a sensible age to determine when a child or young person can be responsible for his or her own health information.[118] The National Children's and Youth Law Centre agreed that it is necessary to set an age at which capacity is assumed for those situations where it is not practical to undertake an independent assessment, but considered that there should be a discretion to rebut the assumption that a child does not have capacity if evidence to the contrary is made available.[119]

60.62 A specific age was suggested in a few submissions. The Obesity Prevention Policy Coalition and Young Media Australia suggested 14 as an appropriate cut-off age in relation to the use of personal information for direct marketing purposes.[120] In youth workshops conducted by the ALRC, there were varying suggestions about the age at which most young people should be able to control access to their health information, although it was generally placed around the age of 14 to 16.[121] The Australian Health Insurance Association suggested that if a lower age cannot be agreed upon, then the age of 18 should be specified in legislation.[122]

60.63 It was also suggested that, where a child or young person does not have the capacity to make appropriate decisions about the handling of personal information, responsibility for making the decisions should fall to the parents.[123]

Health information

60.64 The collection and disclosure of health information raised high levels of concern for young people involved in the ALRC youth workshops. There was a sophisticated understanding of the balancing issues: the need to provide confidential medical advice to young people; the need to ensure the ongoing safety and well being of young patients; the interests and responsibilities of parents; and the professional obligations of the medical profession. There was generally an expectation, however, that any young person who made a decision to seek medical advice on his or her own should be able to assume that the medical professional would maintain confidentiality. Concern was expressed in a number of submissions that individuals under the age of 18 would be

---

116 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007.

117 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

118 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

119 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

120 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.

121 See discussion on youth workshops conducted by the ALRC in Ch 59.

122 Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

123 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.

unable to obtain the proposed Health and Social Services Access Card. Such a cut-off would affect access to health services.[124]

60.65 Decisions about the collection and disclosure of personal information in the context of medical advice and treatment were clearly seen as areas where individual assessment of the decision-making capacity of the child or young person is appropriate.[125] There was support for the guidance set out in the OPC's *Guidelines on Privacy in the Public Health Sector*, which highlights individual assessment of the capacity of children and young people to make privacy decisions.[126] There were also concerns, however, that education and training are required to ensure appropriate implementation of the guidelines.[127]

60.66 There was some support for the position of the AMA that, if a child or young person can make autonomous decisions regarding medical treatment and wishes that treatment to remain confidential, the doctor should respect that decision.[128] The National Health and Medical Research Council suggested this approach should be a legislative requirement.[129] It was stressed in some submissions, however, that the assessment of an individual's capacity to consent to medical treatment must be considered separately to a decision regarding disclosure of his or her personal information. The individual may be unable to consent to the medical treatment (particularly where it is of an invasive nature or has serious consequences), but have the capacity to determine that the practitioner should not disclose the fact and details of the visit.[130]

60.67 This distinction is considered to be even more crucial in the move to a national electronic health record, which may involve decisions to opt in or opt out of the system, or relating to who should have access to the record.

---

124 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007. While the exposure draft Bill does suggest that an individual under the age of 18 is not entitled to an access card, supporting literature notes that, consistent with the existing situation, an individual aged 15 and over will be able to obtain an access card without parental permission: Australian Government Office of Access Card, *Fact Sheet—People Under 18 Years of Age* <www.accesscard.gov.au> at 1 August 2007.

125 Individual assessment may not be practical in the health insurance context: Australian Health Insurance Association, *Submission PR 161,* 31 January 2007.

126 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

127 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

128 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

129 National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

130 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007.

> The requirement of health practitioners to assess the capacity of a young person to consent to an electronic health record has raised particular concerns. Assessing a young person's capacity to make decisions about the handling of their personal and health information … is different to assessing a young person's capacity to make decisions about their healthcare or medical treatment. Therefore is the use of 'standard clinical practice' appropriate? The distinction between capacity to make decisions about privacy, and capacity to make decisions about healthcare needs to be more clearly articulated in any electronic health record implementation.[131]

Possible models for assessing capacity

60.68 The New South Wales Law Reform Commission (NSWLRC) is dealing with similar issues in its current inquiry on the consent of minors to medical treatment. The NSWLRC has identified problems, in particular what some see as a lack of clarity and certainty, with the existing common law position. An individual under the age of 18 can legally consent to medical treatment if he or she is capable of comprehending the nature and consequences of the treatment.[132] The NSWLRC set out five alternate models involving the assessment of consent:

- according to each young person's capacity to understand;
- by fixing a general cut-off age;
- according to the young person's age *and* capacity to understand—for example, by deeming that young people over a certain age have legal capacity, and under a certain age do not have capacity, and for an age bracket in between which would require individual assessment of capacity;
- according to the type of medical treatment—for example, by setting certain ages of legal capacity in relation to treatments such as contraception, termination of pregnancy, drug and alcohol services, or mental health; or
- according to specific groups of young people—for example, by deeming young people who are married, parents themselves, living independently or homeless to have legal capacity.[133]

60.69 A selection of these elements could be combined in an alternative model. The NSWLRC has yet to choose which model, if any, to recommend.[134]

60.70 While this Inquiry is not focusing on consent to medical treatment, the same options arise in relation to assessing capacity to make decisions about an individual's

---

131 Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007.

132 The common law situation is subject to the *Minors (Property and Contracts) Act 1970* (NSW) s 49 and *Guardianship Act 1987* (NSW) pt 5.

133 New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004), Ch 3.

134 The NSWLRC is expected to complete its report on this project by the end of 2007.

personal information. As the circumstances and consequences of these decisions may differ greatly, a different approach may be justifiable under the *Privacy Act*.

60.71 Research on the decision-making capacities of children and young people, international law as reflected in CROC, and recent case law all support individual assessment of capacity. This approach is consistent with the existing regime understood and applied under the *Privacy Act,* and in other privacy legislation in Australia. There is also strong support in the community for continuing this approach. Further, a model that involves communicating with a child or young person to help him or her to understand the nature and consequences of a decision is the best model for involving children and young people in decision-making processes, even where the child or young person is found to be incapable of making the decision on his or her own. The assessment process lends itself to involving parents, guardians or other support adults, so that the child or young person receives support whether he or she is capable or incapable of making an independent decision.

60.72 The ALRC was also made aware, however, that there are practical limitations and difficulties with this approach. Individual assessment presupposes that it is possible to engage with the individual. It also requires that the person making the assessment is suitably qualified to provide support and make an appropriate judgment about the capacity of the individual to understand the nature and consequences of the decision. While such a situation generally exists in a doctor-patient relationship, it does not exist in a wide variety of circumstances involving decisions regarding an individual's personal information. Such circumstances include:

- completing an online form with personal information in order to access subscriber-only parts of a website, where the conditions of access (set out on the website) include allowing the company to use the personal information for marketing purposes;

- providing staff at a gym with a form containing details of medical conditions suffered by an individual;

- agreeing over the phone to participate in a survey, and disclosing personal information during the phone interview;

- completing a form agreeing to the use by an organisation of an individual's personal information held by the organisation for research purposes; or

- sending a letter or email to an agency, or completing an online form, requesting access to a record containing the individual's personal information.

60.73 In many of these situations, the agency or organisation may not be aware of the age of the individual it is engaging with, let alone able to make an assessment

regarding the capacity of the individual to understand the nature and consequences of the decision. While the individual in each scenario may appear to consent to the collection or disclosure of, or access to, his or her personal information, the agency or organisation does not know whether the individual understands fully the consequences that may arise from the decision. At present, in the absence of making a one-on-one assessment concerning the capacity of an individual under the age of 18, there is no guidance on how to handle personal information in these situations.

60.74 Setting a minimum age at which individuals are assumed to be able to make decisions under the *Privacy Act* would enhance clarity and simplicity. So long as an agency or organisation can establish that an individual is over the cut-off age, no assessment of capacity would be required. The agency or organisation would still be subject to the relevant requirements to inform individuals of certain circumstances relating to collection in accordance with the proposed 'Specific Notification' principle, but further inquiry as to whether the individual understands the nature and consequences of the decision would not need to be undertaken.

60.75 Setting a minimum age also would have the benefit of protecting those under that age, by requiring an authorised representative to make decisions on their behalf.[135] This would be appropriate where there are serious or possibly negative consequences of a decision regarding personal information, and the child or young person is not capable of giving appropriate consideration to those consequences. An authorised representative would be required to make, or refuse to make, the decision on behalf of the child or young person, and ensure the child or young person is supported in all the circumstances.

60.76 The simplicity of the minimum age solution, however, also has the potential to cause injustice. It has been suggested that the application of any age-based legislative provision is arbitrary, and may breach the principle of equality before the law.[136] It is inevitable that, wherever the age barrier is placed, there will be some over the age barrier that do not really have the required capacity in relation to all decisions, and there will be some under the age barrier that would have the required capacity in some situations.

60.77 If a minimum age solution is desirable, the next step is to determine the appropriate age. Research on child development and brain development suggests that the cognitive ability to make independent decisions is generally in place by the age of 14 to 16, but this cognitive ability has not fully matured and individuals of this age will continue to be more susceptible than adults to psychosocial factors. These psychosocial factors will have a differing impact depending on the circumstances in which the

---

135 The term 'authorised representative', and who may be an authorised representative, are discussed further below.

136 J Morss, 'But for the Barriers: Significant Extensions to Children's Capacity' (2004) 11 *Psychiatry, Psychology and Law* 319, 321–322.

decision must be made and the potential consequences of the decision, as well as the circumstances of the individual, including his or her stage of social development, socio-economic status, and the support available and accepted by the individual.

60.78 As canvassed by the NSWLRC, it may be appropriate to consider setting age cut-offs at different points depending on the nature of the personal information involved. For example, decisions regarding health information may require a higher level of capacity than decisions regarding disclosure of an email address for direct marketing purposes.[137] The *Privacy Act* already makes a distinction between sensitive information and other personal information and applies additional protection to sensitive information.[138] It may be appropriate to set a higher minimum age for making decisions relating to sensitive information than to other personal information. While this approach is likely to cause some confusion for agencies, organisations and individuals, the fact that differing requirements already apply to the handling of sensitive information suggests it is possible to implement this approach.

60.79 The NSWLRC also considered that certain categories of young people should be deemed to possess legal capacity, particularly those who, in practice, act independently of parents and guardians. Any situation requiring such individuals to have a responsible person to make a decision on their behalf may be impractical. It would be possible to include such an approach under the *Privacy Act*, although it may not be easy to define the categories and it would require additional administrative steps to prove a certain individual falls within a particular category.

Models used in other jurisdictions

60.80 Most privacy legislation overseas takes the same approach as Australian privacy legislation in assuming all individuals, regardless of age, have the same privacy rights. Some overseas legislation makes provision, however, for determining when a child or young person may make decisions in his or her own right, or for determining who may make decisions on behalf of the child or young person.

60.81 The *Privacy Act 1985* (Canada) and the *Personal Information Protection and Electronic Documents Act 2000* (Canada) are similar to Australian legislation in not making age distinctions. Both Acts provide that rights or actions may be exercised or performed on behalf of a minor by an authorised person. It is assumed that an individual assessment model is used in practice, although there is no guidance on the issue.

---

137 It should be noted that the consequences of access to, and disclosure of, health information may differ from decisions regarding health treatment. This is discussed below.

138 The ALRC proposes retaining this distinction for sensitive information. For the definition of sensitive information, see Ch 3. See Ch 19 for a discussion of the provisions relating to sensitive information in the proposed UPPs.

60.82 The United Kingdom uses a combined individual assessment and minimum age model. Guidance has specified that an individual aged 12 or more is presumed to be of sufficient age and maturity to have the required understanding to exercise a right under the *Data Protection Act 1998* (UK), but that an assessment of capacity should be made.[139]

60.83 The *Privacy Act 1993* (NZ) also uses a combined individual assessment and minimum age approach. The Act gives an agency the power to refuse to disclose information requested by an individual under the age of 16 if the disclosure would be contrary to the individual's interests.[140] There is no further guidance in the legislation or otherwise about assessing the capacity of a child or young person to make decisions under the Act, although an individual assessment approach can be assumed. The exception is in the *Health Information Privacy Code 1994* (NZ), issued under the Act, which provides that, where an individual is under the age of 16, the individual's parent or guardian may make decisions regarding the collection, use and disclosure of health information.[141] As the provision is permissive, it does not preclude a younger individual from making a decision in his or her own right, but suggests that a decision by a parent or guardian will take precedence over that of the individual under the age of 16.

60.84 The *Personal Health Information Protection Act 2004* (Ontario) has a number of interesting provisions relating to capacity, which combine an individual assessment and minimum age approach. Essentially it establishes a regime that assumes a person aged 16 or over can consent to the collection, use or disclosure of personal information in his or her own right. It goes on to provide that a parent, children's aid society or other person with parental responsibility may provide consent on behalf of an individual who is under the age of 16, but not if the information relates to medical treatment about which the individual has made his or her own decision, or child and family services counselling in which the individual has participated on his or her own.[142] However, the provision that parents or others may provide consent on behalf of an individual under the age of 16 is further qualified: if the individual is considered to

---

139 This position is set out in the Act only in relation to Scotland, which otherwise deems that an individual does not have legal capacity until the age of 16: *Data Protection Act 1998* (UK) s 66. This also means that in Scotland an individual aged 16 has legal capacity, and no assessment is required. It was not considered necessary to spell out this position in the legislation in relation to Wales, England and Northern Ireland: United Kingdom Government Information Commissioner's Office, *Data Protection Act 1998 Legal Guidance* (2001), 52.

140 *Privacy Act 1993* (NZ) s 29(1)(d). This also means that there is no power to refuse if the individual is aged 16 or over.

141 *Health Information Privacy Code 1994* (NZ) cl 3.

142 *Health Information Protection Act 2004* (Ontario) s 23(2). Each of these exceptions applies to sensitive areas that are regulated by other legislation dealing with the capacity of the individual to provide consent or participate in his or her own right, namely the *Health Care Consent Act 1996* (Ontario) and the *Child and Family Services Act 1990* (Ontario).

be capable of consenting on his or her own, then the decision of the individual prevails over a conflicting decision of the parent or other substitute decision-maker.[143]

ALRC's view

Combining individual assessment and minimum age approaches

60.85 Based on the scientific research and a human rights approach, the ALRC believes that a system of individual assessment is the fairest and most appropriate way to determine if an individual under the age of 18 has the capacity to make a decision. As far as possible, a system of individual assessment should remain in the *Privacy Act*.

60.86 The ALRC is alert, however, to the impracticalities of imposing an across the board individual assessment approach. Decisions relating to personal information arise in a wide variety of contexts, many of which do not allow for individual assessment by the relevant agency or organisation. At present, in these situations it is assumed that an individual who completes a form, makes a phone call or ticks a box has the capacity to make the required decision regarding his or her personal information. However, the consequences of the decision to allow collection or disclosure of personal information can be significant. In particular, the ALRC considers that, as younger children interact increasingly in the online environment, there is a need to set some limits regarding decision making without assessment of the individual's capacity.

60.87 The ALRC proposes a model that combines individual assessment and a minimum age. In all circumstances where an individual assessment is possible, any individual under the age of 18 should be assessed to determine if he or she has the capacity to make a decision to give consent, make a request or exercise a right of access under the Act. Where individual assessment is not possible, there should be a set age at which a presumption of legal capacity exists, and under which it is presumed the individual cannot make a decision in his or her own right. Even if a presumption is initially adopted, at any time an individual assessment may be conducted and the presumption overridden.

60.88 Where legal capacity is found, either by assessment or by operation of the presumption, the individual has the ability to make decisions in his or her own right, to the exclusion of any other person. Where there is no legal capacity, an authorised representative must make a decision on behalf of the individual. Who this authorised representative should be is discussed below.

60.89 The ALRC considers that this approach has two benefits. First, the individual assessment element brings flexibility and recognises the ways in which cognitive

143 Ibid s 23(3).

capacity develops. Secondly, it provides certainty and practical operation in those situations where individual assessment is not available.

Setting the age of presumption

60.90 In many jurisdictions, the age of presumption of legal capacity has been set at 16, with individual assessment below that age. In the United Kingdom it is 12, with individual assessment to be conducted above that age. If the ALRC's proposals are implemented, the set age will apply where individual assessment is not possible. The set age must provide appropriate recognition of the capacity of the vast majority of people above a certain age, without exposing a large number of individuals to the potential consequences of decision making they are not equipped to deal with.

60.91 The balance between parental authority and the evolving capacities of young people to make decisions on their own also must be considered. The recognition of legal capacity will allow young people above a certain age to refuse to consent to disclosure of personal information to others, including their parents.[144] The recent debate concerning parental access to health information records, outlined above, shows that this topic evokes strong feelings in the Australian community.

60.92 Some overseas and Australian legislation and policies that are focused on the protection of children have set a minimum age at 13, under which parental authority or consent is required before personal information can be collected.[145] These statutes and policies impose protections for children that are in addition to the general privacy principles—the need for such additional protections is discussed below. The ALRC does not consider, however, that 13 is an appropriate age at which to expect all young people to take on the responsibilities and consequences of decision making without supervision.

60.93 Given previous debate in the Australian community, and the latest research which highlights the impact of psychosocial factors on adolescent decision making, the ALRC proposes that the minimum age be set at 15. Fifteen is the age at which a young person is entitled to access a separate Medicare card without parental permission.[146] Under the ALRC's proposal, where an individual assessment is not possible, individuals aged 15 and over will be assumed to have the capacity to make decisions under the *Privacy Act*. Individuals under the age of 15 must have an authorised representative make the decision on their behalf.

---

144 The disclosure will be permissible if this is expected as part of the primary purpose of collection, or a related secondary purpose. See the discussion on this point in relation to school reports below.

145 See, eg, *Children's Online Privacy Protection Act 1998* 15 USCA § 6501 (US); Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001). The Australian Labor Party's proposed amendment to the *Privacy Amendment (Private Sector) Act 2000* (Cth) headed 'Special protection for children' also adopted this cut-off age: Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus).

146 Note the discussion above, which indicates the Government's intention that this will remain the case following introduction of the proposed Health and Social Services Access Card.

60.94 This will have implications for agencies and organisations that deal with young people. Such agencies and organisations may have to establish a system for verifying the age of the individual and, if the individual is under the age of 15, establish alternative methods for communicating directly with an authorised representative. These implications are discussed further below.

Encouraging and facilitating appropriate individual assessment

60.95 The ALRC is aware that setting an age of presumption in the legislation may have a negative effect on the system of individual assessment and, in practice, suggest a general presumption for all decisions regarding personal information. The age of presumption is intended to be a fall back position, only to be imposed where an individual assessment is not possible. To ensure that this approach is adopted, there is a need for guidance that encourages individual assessment to be undertaken properly.

60.96 The first step is to have clearer guidance on the meaning of 'capacity' to make a decision under the *Privacy Act*. A number of other information privacy Acts include provisions that make this kind of statement. The ALRC proposes that the *Privacy Act* include a provision, based on that in the *Health Records Act 2001* (Vic) and draft *National Health Privacy Code*,[147] that clarifies the meaning of capacity. The provision should state that an individual under the age of 18 is considered to be incapable of giving consent, making a request or exercising a right if, despite the provision of reasonable assistance by another person, he or she is incapable of:

- understanding the general nature and effect of giving the consent, making the request or exercising the right; or

- communicating such consent or refusal of consent, making the request or personally exercising the right of access.

60.97 One of the important aspects of the proposed provision is the requirement to provide reasonable assistance to the individual to help him or her understand the nature and effect of the decision and to communicate his or her decision. This reflects the need to involve children and young people in the decision-making process and support them to ensure that their capacity is recognised to its full potential, consistent with arts 5 and 12 of CROC. Often such assistance will be provided as part of the assessment, such as during a doctor-patient consultation, or in an information session about participation in a research project. The assistance does not have to be provided directly by the agency or organisation—in some cases, it may be provided by a parent—but there is an onus on the agency or organisation to ensure that reasonable assistance is available.

---

147 *Health Records Act 2001* (Vic) s 85(3); National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4, cl 4(3).

60.98 The ALRC considers that the OPC should develop and publish guidelines on the handling of personal information of individuals under the age of 18. The guidance should stress that individual assessment is the preferred way to determine capacity under the *Privacy Act*. The guidance may suggest particular scenarios where individual assessment should be used and how an appropriate assessment practice can be established. Further guidance on applying the criteria set out in the proposed legislative provision for determining an individual's capacity would also be useful for agencies and organisations.

60.99 There will also be a need to assist agencies and organisations to understand their obligations to provide reasonable assistance to individuals in understanding and communicating decisions. This should include considering how best to involve parents and others in the decision-making process to support the child or young person.

Making decisions for a child or young person without capacity

60.100 The *Privacy Act* does not provide any mechanism for making decisions on behalf of an individual under the age of 18 who is found to be incapable of making a decision on his or her own behalf. It is assumed that parents or guardians will make these decisions. The ALRC considers there is a need to clarify the position in legislation and ensure that an appropriately defined category of persons is entitled to make decisions on behalf of a child or young person who lacks capacity.

60.101 Chapter 61 looks at adults who are incapable of making decisions on their own behalf under the *Privacy Act*. The ALRC proposes adopting the concept of an 'authorised representative', which is used in the *Health Records Act 2001* (Vic) and draft *National Health Privacy Code*.[148] As discussed in Chapter 61, it is necessary to define clearly the categories of person that may act as an authorised representative of an individual. These categories should include, in relation to a person under the age of 18, a person with 'parental responsibility' for the individual.[149] The term 'parental responsibility' will include parents, guardians and other persons who have parenting responsibilities for the child or young person but exclude a parent who, as a result of a court order, no longer has parental responsibility.[150]

Implementing the age of presumption

60.102 Establishing an age of presumption in the absence of the ability to make an individual assessment under the *Privacy Act* will have implications for agencies and organisations. In such situtations, an authorised representative must be found to make a decision on behalf of the individual. This means the establishment of appropriate

---

148 The term 'authorised representative' is defined in *Health Records Act 2001* (Vic) s 85(6); National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4, cl 1.

149 This category is incorporated into the definition of 'authorised representative' set out in Proposal 61–2.

150 The concept of parental responsibility is used in the *Family Law Act 1975* (Cth). An effective definition of 'parental responsibility' to define a person entitled to act on behalf of a child is set out in Exposure Draft Human Services (Enhanced Service Delivery) Bill 2007 (Cth) cl 4.

mechanisms to determine the age of an individual, and to engage with the authorised representative.

60.103 The experience in the United States with the *Children's Online Privacy Act 1998* (COPPA) and the use of parental consent verification mechanisms for online engagement with individuals under the age of 13 has been largely positive.[151] The system involves a sliding scale that heightens the stringency of the verification requirement where the intended use and disclosure of the personal information involves third parties rather than internal use by the organisation.

60.104 Age and parental consent verification systems are not foolproof. In Australia, most online age verification systems are used in conjunction with sites meant for adults only, such as pornography or liquor sales sites. Some security experts have suggested that any technical solution tough enough to keep children safe would penalise legitimate users who could not be verified.[152] Based on its experience, however, the United States Federal Trade Commission (FTC) considers that COPPA has been effective in providing greater protection to children's personal information online.[153] A number of new initiatives in the United States aimed at protecting children are exploring the use of similar age verification mechanisms.[154]

60.105 Requirements for the operation of age and parental consent verification mechanisms and other aspects of the regime are set out in a Rule made under COPPA. There are extensive penalties for non-compliance with the Rule and the FTC puts significant resources into monitoring and enforcing the Rule.

60.106 At this point, the ALRC does not consider it appropriate to prescribe in legislation how to implement the age of presumption in the *Privacy Act*. Neither is it feasible for the OPC to spend significant resources monitoring compliance by agencies and organisations. It would, however, be an issue for consideration as part of any complaint about a breach of the Act, or as part of an audit of compliance. It is the preliminary view of the ALRC that the OPC should provide guidance to agencies and organisations to assist them to establish appropriate mechanisms and practices for implementing the age of presumption, including establishing appropriate age verification mechanisms and facilitating decision making by authorised representatives on behalf of incapable children and young people.

---

151 Further details of COPPA are set out below in a discussion on children and young people as online consumers.

152 'Trying to Keep Children Safe Online', *The Canberra Times* (Canberra), 7 August 2006, 14.

153 United States Government Federal Trade Commission, 'FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes' (Press Release, 8 March 2006).

154 See, eg, the proposed US federal Debit and Check Card Consumer Protection Act, which aims to protect against the theft of children's identities: M Bosworth, 'Sen Clinton Targets Child Identity Theft', *ConsumerAffairs.Com*, 31 October 2006, <www.consumeraffairs.com>. The Bill was not passed.

60.107 While the OPC should encourage the establishment of age verification mechanisms, the ALRC also notes that they are not without problems. For this reason, the ALRC proposes that the *Privacy Act* contain an appropriate limitation on the liability of agencies and organisations when dealing with individuals aged 14 or under where no individual assessment of capacity has been undertaken. The ALRC considers that if the agency or organisation does not know, or could not reasonably be expected to have known from the information available, that an individual was aged 14 or under, the agency or organisation should be able to rely upon the consent.

60.108 This proposal should not be interpreted as allowing agencies and organisations to plead ignorance in every case due to a failure to establish appropriate age verification mechanisms. Consistent with the approach of the COPPA Rule, it would be appropriate for all agencies and organisations that operate services directed to individuals aged 14 and under—or that otherwise have 'actual knowledge' that they handle the personal information of individuals aged 14 and under—have either a system for individual assessment of capacity, or an age verification mechanism. The proposed limitation on the liability of an agency or organisation would cover the situation where the individual deliberately avoided or misled the agency or organisation, or where an agency or organisation that does not usually handle the personal information of children and young people interacts with an individual under the age of presumption, but there is no information available to suggest the individual is under that age. The ALRC considers the proposed limitation is an appropriate balance that allows for practical implementation by agencies and organisations.

Obligations on agencies and organisations

60.109 One of the themes highlighted in submissions and consultations was a lack of knowledge and experience on the part of agencies and organisations when dealing with children and young people. The ALRC proposes, therefore, a number of practical solutions for raising the level of awareness of the proposed provisions and improving the practical application of the provisions.

60.110 In Chapter 21, the ALRC proposes that agencies and organisations should be required to develop and publish a Privacy Policy that sets out how the agency or organisation manages personal information and how personal information is collected, held, used and disclosed.[155] Agencies and organisations that handle the personal information of individuals under the age of 18 should address how such information is managed in their Privacy Policies. This would include addressing issues such as whether an individual assessment of capacity is carried out and by whom, what age verification mechanisms (if any) are used, and how an authorised representative may act on behalf of an incapable child or young person.

155 See Proposals 21–1, 21–2, 21–4.

60.111 The ALRC also considers that agencies and organisations that regularly handle the personal information of individuals under the age of 18 should ensure that their staff are trained adequately to assess the decision-making capacity of children and young people. Where individual assessments are not routinely undertaken, staff should be made aware of the steps to be taken to determine if an individual is over the age of presumption, and what must occur if an individual is under the age of presumption. It may be appropriate that such training is offered by industry associations, possibly as part of broader training programs aimed at improving staff awareness and practices in relation to personal information.

Proposal 60–1 The *Privacy Act* should be amended to provide that:

(a) an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable (in accordance with the criteria set out in Proposal 60–2) of giving that consent, making that request or exercising that right;

(b) where it is practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, an assessment about the individual's capacity should be undertaken; and

(c) where it is not practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, then the consent, request or exercising of the right to access must be provided by an authorised representative of the individual.

Proposal 60–2 The *Privacy Act* should be amended to provide that an individual aged under 18 is incapable of giving consent, making a request or exercising a right if, despite the provision of reasonable assistance by another person, he or she is incapable, by reason of maturity, injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

(b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.

Where an individual under the age of 18 is considered incapable of giving consent, making a request or exercising a right, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of that individual.

Proposal 60–3 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and their authorised representatives in decision-making processes;

(b) situations where children and young people are capable of giving consent, making a request or exercising a right on their own behalf;

(c) practices and criteria to be used in determining whether a child or young person is incapable of giving consent, making a request or exercising a right on his or her own behalf;

(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and

(e) the requirements to obtain consent from an authorised representative of a child or young person in appropriate circumstances.

Proposal 60–4 The *Privacy Act* should be amended to provide that an agency or organisation will not be considered to have acted without consent if it did not know, and could not reasonably be expected to have known from the information available, that an individual was aged 14 or under, and the agency or organisation acted upon the consent given by the individual.

Proposal 60–5 An agency or organisation that handles the personal information of individuals under the age of 18 should address in its Privacy Policy how such information is managed.

Proposal 60–6 An agency or organisation that regularly handles the personal information of individuals under the age of 18 should ensure that its staff are adequately trained to assess the decision-making capacity of children and young people.

Specific privacy issues affecting children and young people

60.112 In the Issues Paper, *Review of Privacy* (IP 31), the ALRC identified a number of areas where privacy issues arise for children and young people.[156] The particular issue of photographs is dealt with in Chapter 59.

Online consumers and direct marketing issues

60.113 Personal information collected in the online environment is subject to the same laws as any other personal information. This chapter focuses on personal information collected in the online environment, such as through registration pages, survey forms, order forms, and online contests. Chapter 6 deals with technology that can be used to capture personal information in ways that are not obvious to the online consumer, such as by using cookies or web bugs, and security issues in the online environment. Chapter 59 deals more specifically with the situation where a child or young person, or a third party, chooses to disclose personal information on a social networking site.

60.114 The internet is an integral part of modern marketing techniques. Given their familiarity and high usage of the internet, and their significant consumer power,[157] it is not surprising that this medium is used to target children and young people.

> The World Wide Web has provided children with abundant new opportunities for learning, communicating and playing. But parents and children need to be aware that the Internet has joined television, radio and print as a key component of today's marketing campaigns and many use consumer information to build individual relationships. Children are often more cyber-savvy than their parents. But they also have a trusting and curious nature that may lead them to give out personal information without realising it.[158]

60.115 There is extensive literature that addresses the particular susceptibilities of children as consumers.[159] When combined with a medium that is often used by children and young people with little or no supervision, concerns arise about the privacy of children and young people as consumers using the internet.

---

156 See Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [9.25]–[9.92].

157 See Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [2.25]–[2.28], [11.1]–[11.2].

158 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 1 August 2007.

159 See, eg, D Kunkel and others, *Report of the APA Task Force on Advertising and Children* (2004) American Psychological Association; R Stanton, 'Into the Mouths of Babes: Marketing to Children' (Paper presented at Cutting Edge: Food and Nutrition for Australian Schools Conference, Brisbane, 18 April 1998); S Beder, *Marketing to Children* (1998) University of Wollongong <www.uow.edu.au/arts/sts/sbeder/children.html> at 1 August 2007; Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997), [11.60]; Federal Bureau of Consumer Affairs, *Final Report: Advertising Directed at Children* (1995).

Online privacy regulation in Australia

60.116 The *Privacy Act* does not distinguish between the application of privacy principles in the online environment and their application in any other area. All agencies and organisations subject to the *Privacy Act* must comply with the IPPs or NPPs in relation to the handling of personal information over the internet. There is some criticism, however, of the operation of the privacy principles in the online environment.

> The fact is that, under existing Australian law, individuals have almost no privacy 'rights' in the online environment and even the few rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced. The lack of rights arises from a combination of factors, including but not limited to, uncertainty regarding the definition of 'personal information'; no requirement to obtain consent before collecting personal information; use of bundled 'consents' including to disclose information to unspecified 'partners'; the small business exemption; and/or technological developments.[160]

60.117 The more general issue of regulation of the internet is addressed in Chapter 6. The ALRC does not propose, however, that privacy in the online environment be regulated separately from other environments. The same set of UPPs is proposed to apply regardless of the medium. The proposed UPPs will have the flexibility and adaptability to apply to the multitude of circumstances in which agencies and organisations must take account of individuals' privacy rights, including technological developments that impact on privacy.

60.118 It is also possible for industries to develop their own standards or guidelines, consistent with the *Privacy Act*, that address particular online privacy practices, including with respect to the privacy of children and young people. For example, the following initiatives relating to online privacy have been developed in Australia:

- The OPC has issued *Guidelines for Federal and ACT Government World Wide Websites* which encourage best privacy practice for websites.[161] Guideline 1 recommends that a privacy policy be prominently displayed on the website.

- The Internet Industry Association (IIA) has developed a Privacy Code of Practice, which is currently under consideration by the OPC.[162] The Code includes a specific provision requiring that a legal guardian provide consent on

---

160 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004.

161 Office of the Federal Privacy Commissioner, *Guidelines for Federal and ACT Government World Wide Websites* (1999). Similar guidelines exist in relation to Victorian, South Australian and Northern Territory government agencies: Office of the Victorian Privacy Commissioner, *Website Privacy—Guidelines for the Victorian Public Sector* (2004); Privacy Committee of South Australia, *Privacy Guidelines for South Australian Government World Wide Websites*; Northern Territory Government Department of Corporate and Information Services, *NT Government Website Guidelines* (2001).

162 The 2001 draft version of the Code, which was circulated for consultation prior to submission to the OPC in March 2003, can be found at <www.iia.net.au>.

behalf of an individual under the age of 13 prior to disclosure of sensitive information collected from or about the child.[163]

- The Australian Direct Marketing Association publishes tips on helping parents to safeguard a child's privacy online, and plans to introduce guidelines on children's privacy that will be compulsory for its members.[164]

60.119 Individuals may adopt various informal methods to avoid improper use of their personal information collected in the online environment, such as providing false information when filling in forms, using pseudonyms and using temporary email accounts.[165]

Online privacy regulation in the United States

60.120 While the United States does not have federal legislation for the online privacy of adult consumers, it does have federal online privacy legislation dealing specifically with children. Based on the recommendations of the FTC,[166] COPPA was passed by the United States Congress in 1998 with a requirement that the FTC issue and enforce rules concerning children's online privacy.

60.121 The COPPA Rule, which came into effect in April 2000, aims to give parents control over what information is collected from their children online. The Rule applies to operators of commercial websites and online services directed to individuals under the age of 13 that collect personal information from children, and to operators of general websites with 'actual knowledge' that they are collecting information from individuals under the age of 13. Foreign run websites must comply with COPPA if they are directed to children in the United States. Under the Rule, operators are required to:

- post a clear and comprehensive privacy policy on their websites;

- provide notice to parents and, with limited exceptions, obtain verifiable parental consent before collecting personal information;

---

163 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001), [6.7]. The term 'child' is defined in [5.1].

164 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 1 August 2007.

165 In a 2004 Australian survey of community attitudes towards privacy, three in ten respondents admitted to having provided false information when filling out a form online, with 53% of 18–24 year old respondents admitting to this behaviour. Thirty-eight per cent of all respondents, and 67% of 18–24 year olds, indicated they use temporary email accounts: Roy Morgan Research, *Community Attitudes Towards Privacy 2004 [prepared for Office of the Privacy Commissioner]* (2004), 64, 66. The ALRC proposes greater recognition of the choice to remain anonymous or use a pseudonym: see Proposals 17–2, 17–3.

166 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998).

- give parents the choice to consent to the collection and use of personal information about their child;

- provide parents with access to their child's personal information to review or have it deleted;

- give parents the opportunity to prevent further collection or use of the information; and

- maintain the confidentiality, security and integrity of information they collect from children.

60.122 The FTC has a sliding scale approach to obtaining verifiable parental consent, with the requirements for obtaining consent becoming more rigorous where the intended use of the information involves disclosure to third parties rather than internal use. Where the information is to be used for internal purposes only, verifiable parental consent can be obtained through the use of an email message to the parent, coupled with additional steps to provide assurances that the person providing the consent is, in fact, the parent. More rigorous methods specified in the Rule include: fax- or mail-back forms; credit card transactions; staffed toll-free numbers; digital certificates using public key technology; and emails accompanied by a PIN or passwords.

60.123 Website operators who violate the COPPA Rule can be liable for civil penalties of up to US$11,000 per violation. The FTC has undertaken an active enforcement approach to COPPA, including 11 successful enforcement cases between 2000 and 2004,[167] and the publication of a survey of the compliance levels of 144 key United States websites.[168] In March 2006, after a public review of the Rule, the FTC announced that the COPPA Rule had succeeded in providing greater protection to children's personal information online, and that the Rule—complete with the sliding scale—was to be retained without amendment.[169]

---

167 All of these cases were settled. For details see the FTC website: United States Federal Trade Commission, *Privacy Initiatives* <www.ftc.gov/privacy/privacyinitiatives/children_enf.html> at 23 August 2007. See also details of a recent settlement against social networking site Xanga.com: D Caterinicchia, 'Xanga Settles with FTC for $1 Million', *Houston Chronicle* (online), 7 September 2006, <www.chron.com>.

168 Conducted one year after commencement of the COPPA Rule, the FTC found that 90% of the surveyed websites provided a privacy policy that complied with the basics of the Rule. However, more than half of the websites did not fully implement other aspects of the Rule—for instance, the prohibition on operators making a child's participation in an online activity conditional on the child providing more information than is reasonably necessary to participate in that activity, and the provision requiring parents to be informed of rights to review, delete and refuse further collection and use of their child's personal information: United States Government Federal Trade Commission, *Protecting Children's Privacy Under COPPA: A Survey on Compliance* (2002), i–ii.

169 United States Government Federal Trade Commission, 'FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes' (Press Release, 8 March 2006).

60.124 There have, however, been criticisms of the COPPA Rule and how it has operated in practice. These include that:

- non-profit organisations are not covered by COPPA;[170]
- operators of general websites do not have to comply with COPPA without 'actual knowledge' of the age of the child, and so can circumvent the Rule merely by not asking the age of the person submitting personal information;[171]
- it is easy for children to circumvent the law by lying about their age, or opening email accounts in their parents' names and giving consent on their own behalf;[172]
- the substantial burden of complying with COPPA has forced many websites simply to eliminate children's programming;[173] and
- even those websites complying with the COPPA Rule do not necessarily comply with the spirit of the law, and most existing privacy policies are too complex for children or parents to understand.[174]

Submissions and consultations

60.125 Few submissions dealt directly with the issue of children as consumers using the internet, and whether there should be any particular provisions for the protection of young consumers in the online environment.[175] The Queensland Commission for Children and Young People and Child Guardian considered that children and young people should be required to give informed consent before any personal information is collected from them online.

60.126 The Obesity Prevention Policy Coalition and Young Media Australia (OPPC and YMA) provided a submission that focused on the problems of direct marketing aimed at children and young people.[176] Although the concerns about direct marketing arise regardless of the media involved, the increasing use of technology to engage with children and young people was seen as a concern.

---

170 K Howard and Y Lim, 'Protection of Children in the Virtual World' (2005) 2 *Privacy Law Bulletin* 17, 19.

171 Ibid, 19.

172 M Hersh, 'Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet' (2001) 28 *Fordham Urban Law Journal* 1831, 1870.

173 K Walker, 'The Costs of Privacy' (2001) 25 *Harvard Journal of Law & Public Policy* 87, 125.

174 J Turow, *Privacy Policies on Children's Websites: Do They Play By the Rules?* (2001) Annenburg Public Policy Center of the University of Pennsylvania, 12.

175 Although see discussion in Ch 59 about children and young people as users of social networking sites.

176 Obesity Prevention Policy Coalition and Young Media Australia, *Submission PR 144,* 25 January 2007.

> In our view, protecting children from interference with their privacy through direct marketing is becoming increasingly important in light of children's increasing use of the internet, email and SMS, and advertisers' widespread use of these technologies to market products directly to children … We are particularly concerned about direct marketing using these technologies because, unlike television, these technologies enable marketers to interact directly with children. Direct marketing using these technologies intrudes directly into children's personal space, and provides marketers with unsupervised access to children.[177]

60.127 The OPPC and YMA cited research indicating that children are more susceptible to commercial influence, and that they are unfairly manipulated by direct marketing.[178] Many children and young people do not have the capacity to make appropriate decisions regarding the disclosure of personal information in a direct marketing context. Further, direct marketers are unlikely to have the kind of contact with children or young people required to make any individual assessment about capacity. It was also noted that direct marketers have a vested interest in assuming that consent is informed and freely given.

60.128 The OPPC and YMA therefore suggested that direct marketers should be prohibited from collecting or using information without the express, verified consent of the child's parent if they know, or would be reasonably likely to know, that it is about an individual under the age of 14. It was proposed that the express, verified consent should be able to be provided through a signed form sent by mail or fax, provision of a credit card number or electronic signature, or calling a toll-free number staffed by trained personnel. It was also suggested that there be a prohibition on making consent to use personal information for direct marketing purposes a condition of entry to a competition, promotion or other activity if the entrant is under the age of 14. The OPPC and YMA provided a number of examples where this condition of entry has been used in competitions or clubs aimed at children in Australia.

ALRC's view

60.129 Given the concerns raised about collection of personal information about children and young people for direct marketing purposes, particularly in the online environment, there is a need to consider whether the *Privacy Act* or related legislation should contain additional protections for children and young people that modify the general application of the privacy principles.

60.130 One option is to adopt a model based on COPPA. Many aspects of COPPA apply general privacy regulatory measures that are necessary due to the absence of general information privacy legislation in the US. These requirements, including posting privacy policies on websites, rights of access and correction, and obligations to maintain the confidentiality, security and integrity of collected personal information,

---

177 Ibid.

178 See, in particular, D Kunkel and others, *Report of the APA Task Force on Advertising and Children* (2004) American Psychological Association.

will apply under the proposed UPPs to all personal information, not only to personal information about children.[179]

60.131 The major additional protections provided by COPPA, which appeal to some in the Australian community, are the requirements to obtain verifiable parental consent before collecting any personal information from an individual under the age of 13, and giving parents the opportunity to prevent further collection or use of the information. This was the basis of the proposed amendment for the 'special protection for children' put forward by the Australian Labor Party during debate on the Privacy Amendment (Private Sector) Bill 2000 (Cth), although the proposal was not limited to online activity as it is in COPPA.[180]

60.132 The suggestion for additional protections when collecting personal information from children stems from concerns that children are unable to make an informed choice before providing personal information to an agency or organisation. For example, a child is more likely than an adult to complete an online form and provide personal information in order to continue to play a game or enter a competition without giving appropriate consideration to the intended use of the personal information. Even where a child stops to consider the consequences, he or she is less likely than an adult to find and understand the agency's or organisation's privacy policy. Combined with the knowledge that children are interacting regularly in the online environment, sometimes without adult supervision, this is seen as a concern by some stakeholders.

60.133 Under the proposed UPPs, it is not necessary to obtain an individual's consent to collect his or her personal information except in relation to sensitive information where no other exception allows for collection without consent. While consent is not required for collection of non-sensitive personal information, an individual can often choose to take steps to prevent an agency or organisation from collecting that personal information. This contributes to the ALRC's proposal that agencies and organisations should be required to collect personal information directly from an individual wherever reasonable and practicable.[181] The ALRC also makes a number of proposals aimed at improving the extent and clarity of information made available to individuals about how their personal information will be handled.[182] These proposals, however, will not be of assistance to a child who is incapable of understanding and synthesising the information so as to make informed choices.

---

179 See Ch 21.

180 Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 November 2006, 20302 (N Bolkus).

181 Proposal 18–1. This requirement exists in NPP 1.4 in relation to organisations, and the ALRC proposes extending the requirement to apply to agencies.

182 See Ch 20.

60.134 On the other hand, there are practical reasons why the general privacy principles do not require consent to every collection of personal information. There needs to be a balance between privacy protection and the practical operation of services and businesses. The proposed UPPs are designed to build in protections where they are required while still allowing for the appropriate flow of information. This may require agencies and organisations to seek consent from individuals where there are particular risks, such as before the collection of sensitive information, and before a use or disclosure that is not consistent with the primary purpose of collection, or otherwise covered by the carefully crafted exceptions to the proposed 'Use and Disclosure' principle. General protections relating to data quality and security apply to all personal information regardless of the way in which it was captured.

60.135 In general, it is the preliminary view of the ALRC that the balance provided in the proposed UPPs between privacy protection and the free flow of information is appropriate and gives adequate protection to personal information about children. In addition, the ALRC's proposal to require the assessment of the capacity of an individual to provide consent or otherwise to require an authorised representative to provide consent on behalf of an individual aged 14 or under provides protections that are not available at present.[183]

60.136 The ALRC notes particular concerns about direct marketing, and that some organisations running competitions aimed at children require consent to use personal information for direct marketing purposes as a condition of entry to the competition. There is, however, a limitation in relation to the use by organisations of personal information about children for direct marketing purposes. While consent is not required to collect personal information, it is required before personal information can be used for direct marketing purposes. In practice, this consent to use is generally obtained at the point of collection and, if consent is refused, would often leave an organisation with little reason to collect the personal information. Under the ALRC's proposals, the consent of an authorised representative will be required if the individual is aged 14 or under. While the proposed 'Direct Marketing' principle allows an organisation to use personal information for direct marketing purposes where obtaining consent is impracticable, the ALRC suggests that guidance should indicate clearly that the need to establish an age and parental consent verification mechanism should not be considered impracticable if the organisation is knowingly handling the personal information of individuals aged 14 and under.

60.137 Questions may be raised about whether direct marketing to children is, of itself, undesirable. The OPPC and YMA presented evidence highlighting that children, for developmental reasons, are less able to resist commercial influence and that the risks to children are heightened when combined with technology that enables organisations to contact children directly. The proposals in this Discussion Paper would help to protect the privacy of personal information about children, and would

183 See Proposal 60–2 above.

assist to limit unsupervised contact by direct marketers. It is not appropriate, however, to prohibit direct marketing to children through information privacy law.

60.138 On balance, it is the preliminary view of the ALRC that there is no need to enact additional privacy protections for children. Further guidance is needed, however, to clarify the operation of the proposed 'Direct Marketing' principle to ensure that appropriate protection and requirements to obtain consent from an authorised representative are implemented in relation to individuals aged 14 and under.[184]

Schools

60.139 School is the most significant institution in the lives of the majority of children and young people. Schools collect and hold a vast array of personal information regarding children and young people, including names, addresses, family information, subjects studied, grades and behavioural information. Schools will often hold health information about children and young people, either collected directly from the child or young person (or their parents or guardians), or collected as part of a service offered within the school, such as visits to a school dentist, nurse or counsellor. Photos and videos of children and young people taken by the school also fall within the definition of personal information.

60.140 With the exception of the ACT, government schools are not covered by the *Privacy Act* but are subject to any state or territory privacy legislation or scheme covering the public sector. Some states and territories have a privacy policy or privacy code that applies to all of their schools.[185] Further, many schools have developed policies or practices dealing specifically with the publication on their websites of photographs or videos depicting children and young people.[186]

60.141 Private schools are covered by the *Privacy Act* unless they fall within the small business exemption.[187] Even smaller private schools are likely to be partly covered by the *Privacy Act*: information relating to the provision of a health service, which includes physical education classes or fitness instruction as well as services provided by nurses and other health professionals, is regarded as 'health information'

---

184 Guidance of this kind is proposed in Proposal 23–6.

185 See, eg, South Australian Government Department of Education and Children's Services, *SA Government Schools and Children's Services: Information Privacy Statement* which sets out that the disclosure of personal information is regulated by the South Australian *Information Privacy Principles* and that access to information about a person may be requested by that person or a parent or guardian of that person.

186 See, eg, Curriculum Materials Information Services, *Protecting Student Privacy* Department of Education and Training Western Australia <www.det.wa.edu.au/education/cmis> at 1 August 2007, which suggests that parental consent should be sought when photographs or digital images of students are to be used outside the classroom environment, eg, in the local community newspaper, or on a website or CD-ROM promoting the school.

187 Note that the ALRC proposes the removal of the small business exemption from the *Privacy Act*: see Proposal 35–1.

and is regulated by the Act.[188] The OPC takes the view that, in most instances, private schools and colleges are covered by the Act and should comply with the NPPs.[189]

60.142 One of the key issues relating to access to the records of a child or young person is whether the school can disclose a record to a parent or guardian. In the private school context, it is generally the parents or guardians who enter a contract with the school to provide a service. Schools subject to the NPPs, however, must only disclose personal information regarding the child or young person consistently with the NPPs.

60.143 Advice from the OPC suggests that most personal information collected by a private school may be disclosed to parents as, under NPP 2.1(a), students would, in most cases, reasonably expect disclosure of the information to parents. The OPC indicates that disclosure of school reports and also material not related to education, such as health information or counselling records, would generally be expected.[190] For older students, however, these expectations may differ in relation to some records containing sensitive information. The OPC suggests that it is good practice, particularly in respect of older students, for schools to have a policy on disclosure of records that is made available to parents and students.[191] A number of policies relevant to government schools suggest that parents should have access to their child's records, at least until the child turns 18.[192]

60.144 School counselling is an area where privacy concerns arise. Most secondary schools provide a school counsellor on a full-time or part-time basis, and most primary schools have access to a school counsellor. While school counsellors are an important resource for young people, research suggests that a key reason why young people do not use them is because of concerns regarding confidentiality.[193] Policies regarding the confidentiality of school counselling services vary. All counsellors in any environment are subject to restrictions on the confidentiality of their communications, including mandatory reporting obligations under child protection and communicable diseases

---

188 Office of the Privacy Commissioner, *FAQs: Are Private Schools and Colleges Covered by the New Private Sector Provisions* <www.privacy.gov.au/faqs/cf/q3.html> at 1 August 2007.

189 Ibid.

190 Office of the Privacy Commissioner, *FAQs: Can Private Schools Disclose Non-education Related Personal Information about Students to Their Parents?* <www.privacy.gov.au/faqs/cf/q6.html> at 1 August 2007; Office of the Privacy Commissioner, *FAQs: Can Parents Whose Children Attend a Private School/College Still Get Access to Their Children's School Reports?* <www.privacy.gov.au/faqs/ypr/q15.html> at 1 August 2007. The Office of the Victorian Privacy Commissioner has given similar advice in relation to school reports in Victoria: Office of the Victorian Privacy Commissioner, *Privacy and School Reports: Fact Sheet 02.02* (2002).

191 Office of the Privacy Commissioner, *FAQs: Can Private Schools Disclose Non-education Related Personal Information about Students to Their Parents?* <www.privacy.gov.au/faqs/cf/q6.html> at 1 August 2007.

192 See South Australian Government Department of Education and Children's Services, *SA Government Schools and Children's Services: Information Privacy Statement* and ACT Department of Education & Training and ACT Children's Youth & Family Services Bureau, *School Policy: Access to Student Records: Policy and Implementation Guidelines* (2003).

193 W Reid, *School Counselling: A Client Centred Perspective* (1996) Kids Help Line, 10.

laws. As employees of a school or education department, however, many counsellors are torn between maintaining confidentiality and the demands of principals and teachers who feel they have the right to know what is affecting a particular student.[194]

Submissions and consultations

60.145 A number of bodies that act on behalf of children and young people made submissions highlighting concerns about privacy in schools. The concerns included:

- inconsistencies in privacy practices at different schools;[195]
- increasing amounts of personal information being collected by schools for risk management purposes. It has been suggested that while the collection is being done with consent, there are increased dangers of inappropriate disclosure;[196]
- examples of private schools contracting away a student's right to privacy in a standard form agreement with fee paying parents for the provision of education to the student;[197]
- intrusive practices that breach privacy, sometimes supported by school policies;[198]
- the interpretation of NPP 2 by schools to justify disclosure of personal information about students to parents without consent on the basis that it is a disclosure reasonably expected by the student—the views, age and maturity of each student should be taken into consideration, and the student given the opportunity to object to disclosure in particular circumstances;[199]
- the need for funding for schools to develop and implement clear privacy policies, including informing parents of the privacy rights of students, and development of a school privacy audit tool to measure how effectively students' privacy is being respected and protected;[200] and

194 Ibid, 8.
195 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.
196 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
197 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.
198 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.
199 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.
200 Youth Affairs Council of Victoria Inc, *Submission PR 172,* 5 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007.

- the need for stronger sanctions for schools failing to adhere to privacy laws.[201]

60.146 The Australian Privacy Foundation raised concerns about the increasing use of technology in schools involving collection and storage of personal information, such as fingerprinting for school library services, swipe cards for monitoring attendance, and the use of closed-circuit television (CCTV) for security purposes.[202] The Foundation noted these are often introduced for administrative convenience with little regard for privacy concerns, and that further consultation on such developments should be undertaken before they are introduced.

60.147 The National Catholic Education Commission (NCEC) and the Independent Schools Council of Australia (ISCA) provided the ALRC with a copy of their *Privacy Compliance Manual*, which was developed in conjunction with the OPC.[203] The NCEC and ISCA indicated that the Manual has been an effective tool in assisting non-government schools to comply with the *Privacy Act*, and that there have been very few expressions of concern to those bodies about infringements of privacy.

60.148 The NCEC and ISCA indicated that schools rely on the consent of a parent (regardless of the age of the student) to collect such information. On the issue of disclosure of personal information about students to parents, the NCEC and ISCA indicated that, in many circumstances, personal information collected about a student will be disclosed to parents where the disclosure is normally expected given the primary or related secondary purpose for which the information was collected.[204] It was also noted, however, that there may be circumstances where the information is not disclosed to parents, such as the results of psychological testing, or where there are allegations of domestic abuse. The NCEC and ISCA suggested that schools use a test of what is in the best interests of the student to determine whether personal information should be disclosed.

60.149 The NCEC and ISCA stated that it should be recognised that there are a number of primary factors dictating how personal information may be used and disclosed in a particular situation, including contracts with parents, the welfare of the particular student, and the discharge of the school's duty of care towards the student and other students.[205]

---

201 Youthlaw, *Submission PR 152,* 30 January 2007.

202 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007. See also H Edwards, 'The Digital Finger is Pointing at Truants', *Sun Herald* (online), 22 October 2006, <www.fairfax.com.au>.

203 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007; National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001). Between them, the NCEC and ISCA represent around 2,800 schools in Australia with over 1,000,000 students enrolled in those schools.

204 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

205 Ibid.

60.150 The NCEC and ISCA raised a number of other issues regarding the operation of the *Privacy Act* and the NPPs that make it difficult for schools to comply with privacy laws. They suggested that the existing exceptions to allow refusal of access to an individual's record were too limited to cover the full range of circumstances in which access should be able to be refused.[206] They suggested extended circumstances include where providing access:

- would be inconsistent with the school's duty of care to other students and staff;
- may be detrimental to the safety or well being of a child;
- will be likely to discourage free flow of information between a school and parents or a school and its pupils; and
- may discourage people from providing information in a court of inquiry about possible unlawful activities or other inquiries affecting the well being of pupils.

60.151 The NCEC and ISCA also noted new provisions in New South Wales and Queensland legislation that authorise the transfer between schools of personal information about a student, without consent of the student or parent or guardian, before enrolment of the student in a new school.[207] The purpose of the provisions is to allow the new school properly to assess behavioural issues and consider the health and safety of the transferring student and other students in the school. In the past, this kind of information was not always disclosed to the new school due to privacy concerns. The NCEC and ISCA suggested that such a provision should be included in the *Privacy Act* with the aim of having uniform operation across all Australian states and territories, and in particular covering interstate transfer of students.[208]

60.152 The ALRC notes that a national protocol has been developed through the Ministerial Council on Education, Employment, Training and Youth Affairs (MCEETYA) to provide for transfer of data when students transfer interstate, encompassing both government and non-government schools.[209] The protocol does not

---

206 Ibid.

207 *Education Act 1990* (NSW) pt 5A inserted by the *Education Legislation Amendment Act 2006* (NSW)—the provisions have not yet been proclaimed and are not in operation at present; *Education (General Provisions) Act 2006* (Qld) ss 383–389. The Queensland provisions require that copies of the transferred information be provided to the parent of a student or, in appropriate cases, just to the student, but no consent is required prior to transferring the information: *Education (General Provisions) Act 2006* (Qld) ss 387.

208 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007.

209 The protocol was developed and agreed on by the Australian Government, state and territory education authorities, the independent and Catholic education sectors through MCEETYA. The requirement to use the Interstate Student Data Transfer Note (ISDTN) is set out in the *Schools Assistance (Learning Together—Achieving Through Choice and Opportunity) Act 2004* (Cth) s 31(m). Details of the ISDTN

apply to intrastate transfers. The protocol provides for transfer of personal information from a government school only with the consent of the parent or guardian and, where the student is aged 16 or over, the consent of the student. Consistent with information privacy laws in most Australian jurisdictions, the protocol suggests that transfer may be possible without consent if required to prevent a serious risk to the student or public health and safety. The protocol establishes that consent is not required if a non-government school has a data collection notice that complies with the NCEC and ISCA *Privacy Compliance Manual* advising parents, guardians and students that personal and sensitive information may be disclosed to other schools for administrative and educational purposes.[210]

60.153 The duties of school counsellors was another school-related issue raised in submissions and consultations, and gave rise to conflicting views. Young people involved in the ALRC's youth workshops were adamant that a visit to a school counsellor should be confidential, although many indicated that their impression or experience of school counselling was that it had only limited confidentiality, either because of the physical limitations of seeking advice from counsellors situated within the school, or because of what was seen as 'a breach of confidence' because information had been disclosed to someone else during the experience.[211]

60.154 The NCEC and ISCA considered that counsellors employed by schools and related bodies (such as a Catholic welfare agency retained by the school to provide counselling services) have a duty to inform the school principal if the counsellor becomes aware of information that may affect the health or well being of the pupil, and is relevant to the school performing its contractual duties to provide schooling. The NCEC and ISCA also believed that the records of school counsellors are the same as any other school record, and that the counsellor could be directed to disclose the contents of a discussion to the school principal.[212] The NCEC and ISCA indicated that some counsellors have suggested that this situation should be changed by legislation. The NCEC and ISCA opposed any such change.

---

are available at Ministerial Council on Education Employment Training and Youth Affairs, *Interstate Student Data Transfer Note* <www.mceetya.edu.au/mceetya/default.asp?id=12095> at 1 August 2007.

210 National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001), [7.10.1]. As indicated in the *Privacy Compliance Manual*, the standard form data collection notice is intended to ensure that the individual is reasonably aware of the matters specified in NPP 1.3 and to obtain consent for use and disclosure of personal information that may not be regarded as being for primary or secondary related (or directly related) purposes.

211 This issue was also raised at Children and Young People Issues Roundtable, *Consultation PC 121*, Sydney, 7 March 2007.

212 National Catholic Education Commission and Independent Schools Council of Australia, *Submission PR 85,* 12 January 2007. This is set out in National Catholic Education Commission and National Council of Independent Schools' Associations, *Privacy Compliance Manual* (revised 2004 ed, 2001), 75.

ALRC's view

Privacy policies in schools

60.155 Concerns raised about the handling of personal information in schools appear to stem from a combination of poor practices that are inconsistent with privacy principles, and school policies that provide sometimes questionable interpretations of the privacy principles. The ALRC considers that the proposed UPPs are capable of operating effectively in the school environment and that no specific additional rules are required. There is, however, a need to clarify aspects of the operation of the privacy principles and to ensure appropriate implementation.

60.156 Most schools, education departments and independent bodies representing schools, have privacy policies or more detailed privacy manuals in place. These are essential to provide guidance and some level of certainty regarding the requirements for the handling of personal information to individual schools, and to teachers, students, parents and guardians within the school community. Proposal 21–1 will make development of a Privacy Policy a requirement for every school subject to the *Privacy Act*, and the ALRC supports the development of privacy manuals to provide additional guidance. The ALRC is concerned, however, that some of the content of existing policies and manuals is not wholly consistent with the proposed UPPs and the *Privacy Act*.

60.157 Privacy Policies and manuals in schools should reflect the general approach set out in the ALRC's proposals that individual assessment of a child or young person is the most appropriate way to determine his or her decision-making capacity. Some situations in the school environment should allow for individual assessment—particularly where the information and situation are unique—rather than impose a general administrative rule for all students within the school. Where individual assessment is not appropriate, the ALRC's proposed age of 15 should be adopted as the age from which it is presumed that the young person has the capacity to make a decision regarding his or her personal information.

60.158 This is not to say that every student aged 15 or over should be able to withhold all personal information from his or her parents or guardians. Existing privacy policies and privacy manuals note appropriately that much of the personal information held by schools can be disclosed to parents or guardians as this is expected, either as part of the primary purpose of collection, or a related secondary purpose. School reports are a prime example, and guidance from the OPC supports this interpretation of the privacy principles.[213] School privacy policies should clearly

213 Federal legislation requires, as a condition of federal funding, that schools provide parents of each student school reports twice a year on the progress and achievements of the student: *Schools Assistance (Learning Together—Achieving Through Choice and Opportunity) Act 2004* (Cth) s 32.

describe the kinds of personal information that are collected, the purpose of collection, and situations where the information will be disclosed routinely to parents and guardians.

60.159 This does not mean, however, that the privacy rights of students can be overridden by a Privacy Policy. The ALRC has particular concerns about suggestions that some schools assume that contracts between parents and a school displace the privacy rights of the student. Any Privacy Policy must be consistent with the proposed UPPs and the *Privacy Act* more generally. It is possible that contractual arrangements between parents and a school may contextualise the purpose for which certain information is collected by the school. Use and disclosure must, however, be undertaken consistently with the operation of the proposed UPPs. Privacy Policies can assist to clarify the purpose of collection and, therefore, the intended use and disclosure of certain types of personal information.

60.160 Some concerns were raised that non-compliant schools are not dealt with effectively under the existing regime. This is of concern if, as has been suggested to the ALRC, some school privacy policies and practices are not consistent with the *Privacy Act*. The ALRC has made a number of proposals aimed at improving compliance of agencies and organisations subject to the Act. These proposals would also apply to schools subject to the Act.[214]

Suggested school-specific changes to the Privacy Act

60.161 The NCEC and ISCA made a number of other suggestions for changes to the *Privacy Act* and the privacy principles better to take into account situations that arise in schools. The ALRC has considered some of these suggestions as part of its broader consideration of the 'Access and Correction' principle in Chapter 26. The ALRC's general approach is to ensure that the proposed UPPs have a broad general application with high-level principles wherever possible. Where there is a need for more specific obligations, the ALRC proposes the development of primary or subordinate legislation that covers a particular aspect of privacy or the handling of personal information.[215] The ALRC has identified this need in the areas of credit reporting, health services and research, and in the telecommunications industry.

60.162 The ALRC considers that the proposed UPPs adequately cover the handling of personal information in schools, and there is no need for school-specific provisions in the *Privacy Act* that add to or derogate from the UPPs. The appropriate interpretation of the principles in a school situation can be set out in manuals developed by peak bodies, individual schools or education departments.

---

214 See Chs 42, 46.
215 See Proposal 15–3.

60.163 The ALRC notes the concerns raised by the NCEC and ISCA concerning the transfer of personal information between schools. Steps have been taken to alleviate the problems encountered by schools, through the national protocol developed by MCEETYA for interstate transfers, which clarifies the circumstances in which personal information can be transferred, and the statutory provisions adopted in Queensland and New South Wales, which allow for transfer of personal information without consent of the student or person with parental responsibility. The ALRC acknowledges, however, that outside of Queensland and New South Wales, schools are often unable to transfer personal information without student or parental consent unless the disclosure falls under one of the other exceptions within the proposed 'Use and Disclosure' principle—such as where disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety.[216] While the ALRC agrees with the NCEC and ISCA that this situation would best be remedied through a national approach, the ALRC does not consider that the inclusion of sector-specific amendments to the *Privacy Act* is appropriate, or that it would achieve the desired national consistency.

60.164 It is, however, appropriate to incorporate information about the operation of the MCEETYA interstate protocol for transfer of student data, and any state or territory provision providing for intrastate transfer, into the privacy policies of schools to inform students and those with parental responsibility about the operation of rules for the transfer of personal information.

School counselling

60.165 A particular area where there appears to be conflict and inconsistencies in approach is in relation to the obligations on counsellors to disclose personal information to school management and parents. Counsellors, and students, want as few limitations as possible on the confidentiality of the service, enabling counsellors to develop a level of trust with students and provide an effective service in which the students have confidence. This must be balanced, of course, with the needs of the employer school to meet its obligations to provide support for the individual student, and to protect that student and the broader student body.

60.166 The ALRC considers that the *Privacy Act* and the proposed UPPs contain appropriate exceptions that allow disclosure of personal information without consent of the individual, including in circumstances where there is a serious threat to an individual's life, health or safety; or to public health or public safety. The exceptions do not use school-specific language, but the ALRC considers that they adequately cover situations likely to be encountered in schools.

---

216 Note that the proposed exception differs from the existing exception by removing the requirement that the threat be both serious *and imminent*: see Ch 22 and Proposal 22–3.

60.167 School privacy policies should set out clearly the limits of the confidentiality of school counselling services, and indicate circumstances—consistent with the proposed UPPs and any additional legislative obligations—in which personal information collected by school counsellors will be disclosed to the school management, persons with parental responsibility, and others.

Proposal 60–7 Schools should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:

(a) will be disclosed to, or withheld from, persons with parental responsibility; and

(b) collected by school counsellors will be disclosed to the school management, persons with parental responsibility, or others.

Child care services

60.168 A growing number of Australian children come into contact with formal child care prior to commencing school.[217] As with schools, child care services collect a vast amount of personal information about a child, and his or her family, in order to provide a service.

60.169 A wide range of formal child care services are available, and each has a different structure. They include community-based non-profit services, services administered by local councils, individuals providing care in their own homes, privately owned and managed centres (including some owned by publicly listed companies), and services provided by employers attached to the workplace of parents. Regulation of the sector is shared between the Australian Government and the states and territories.

60.170 The application of privacy laws to the child care sector is confusing.[218] Larger private or non-profit businesses running child care centres are subject to the NPPs, but many smaller centres, most non-profit services and individuals running a service within their own home are exempt from the operation of the *Privacy Act* as a

217 In 2005, 53% of three year olds were receiving some form of formal child care. Overall, for children aged 0–11, formal care (either alone or in combination) was used by 23% of children, up from 19% in 2002 and continuing the upward trend observed since 1996: Australian Bureau of Statistics, *Child Care, Australia, 2005*, 4402.0 (2006).

218 Until 2000, child care service providers that received Commonwealth funding had to enter a contract with the Commonwealth and thus provided services under contract to the Commonwealth, attracting the application of the IPPs. Due to a change in funding arrangements, this is no longer the case.

small business.[219] Some otherwise exempt small businesses, however, may fall within the definition of a health service provider under the *Privacy Act* or state health information legislation. Services operated by a state, territory or local council are subject to any relevant state or territory privacy legislation or scheme.[220]

60.171 National standards have been developed for child care services, and have been utilised to inform child care regulations, funding guidelines and information resources.[221] The degree of implementation has varied between jurisdictions. Each set of standards includes a standard on maintenance of records listing the information (most of which would fall within the definition of personal information) that must be kept confidential, although they differ on when that information may be disclosed.[222] Some child care centres have their own privacy policies in place to govern the collection, use and disclosure of personal information.

60.172 For the administration of payments for the Child Care Benefit scheme, child care services are required to transfer information about child attendances to the Australian Government Department of Families, Community Services and Indigenous Affairs (FaCSIA). It is expected that these requirements will become more rigorous as part of the new Child Care Management System, which is designed to make the industry more accountable.[223] Information held by the Department is subject to the

---

219 Note that the ALRC proposes the removal of the small business exemption from the *Privacy Act*: see Proposal 35–1.

220 For a discussion of the different privacy regimes that may be applicable to a child care service, see K Flanagan, *Privacy in NSW Children's Services* (2002) Community Child Care Co-operative <www.ccccnsw.org.au/facts> at 1 August 2007.

221 See Children's Services Sub-Committee, *Standards for Centre Based Long Day Care* (1993) Australian Government Department of Families, Community Services and Indigenous Affairs; Children's Services Sub-Committee, *National Standards for Family Day Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs; Children's Services Sub-Committee, *National Standards for Outside School Hours Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs. All of the Standards can be found at <www.facsia.gov.au>. These Standards are currently under review.

222 The Standards for centre-based long day care indicate that records should be kept up-to-date and in a 'safe and secure area', that they 'remain confidential' and only made available 'to those who have a genuine interest' in obtaining the record: Children's Services Sub-Committee, *Standards for Centre Based Long Day Care* (1993) Australian Government Department of Families, Community Services and Indigenous Affairs, 5.3.1. The Standards for family day care are similar but only allow that records be made available 'to those who have a lawful right to them': Children's Services Sub-Committee, *National Standards for Family Day Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs, 4.3.1. The Standards for outside of school hours care are silent on the issue of disclosure: Children's Services Sub-Committee, *National Standards for Outside School Hours Care* (1995) Australian Government Department of Families, Community Services and Indigenous Affairs, 5.3.2.

223 The National Child Care Management System will be implemented progressively across child care services from 1 July 2007 to 30 June 2009: Australian Government Department of Families Community Services and Indigenous Affairs, *Child Care Management System* (2007) <www.facs.gov.au> at 1 August 2007.

Privacy Act, and staff are also subject to the confidentiality provisions of the *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth).[224]

Submissions and consultations

60.173 FaCSIA submitted that the specific privacy and secrecy provisions in family assistance law provide adequate privacy protection for personal information transferred to it by child care services.[225] The National Children's and Youth Law Centre indicated that the application of privacy laws is confusing in the area of child care services, given the variety of services, varying regulatory mechanisms and the possible range of applicable privacy laws.[226] The Centre supported a national strategy to review privacy policies and standards in child care services.

ALRC's view

60.174 Most of the concerns about the handling of personal information in child care services stem from the broad range of services available, the varying regulatory structures applied to the services, and the resulting confusion as to the applicable privacy requirements. The ALRC's proposals to harmonise information privacy laws across federal, state and territory jurisdictions will help to reduce the confusion by ensuring that consistent privacy principles apply regardless of the regulatory structure in place for the particular child care service. In the absence of more specific concerns about the handling of personal information in child care services, the ALRC does not propose specific reform in this area.

Media

60.175 In Australia, the acts and practices of a media organisation in the course of journalism are exempt from the operation of the *Privacy Act* if the organisation is publicly committed to observe privacy standards that have been published in writing either by the organisation, or by a person or body representing a class of media organisation.[227] Currently, there are broadcasting codes and standards, which include privacy standards or principles, published separately by the commercial television industry, commercial radio industry, the Australian Broadcasting Corporation, SBS, the Australian Subscription Television and Radio Association and the Community Broadcasting Association of Australia. The Australian Communications and Media Authority (ACMA) has published *Privacy Guidelines for Broadcasters*, which are 'intended to assist broadcasters and members of the public to better understand the operation of the privacy provisions in the various codes of practice'.[228]

---

224 The Department has developed a policy for the disclosure of protected information relating to child care services: Department of Family and Community Services, *Child Care Service Handbook 2005–2006* (2005), App 1.

225 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

226 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

227 *Privacy Act 1988* (Cth) s 7B(4). For further discussion of the 'media exemption', see Ch 38.

228 Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), 1.

60.176 The only set of Australian broadcasting standards or principles that deal specifically with the privacy of children is the *Commercial Television Industry Code of Practice*.[229] For the purposes of the Code, a 'child' means a person under 16 years.[230] Section 4.3.5.1 states that:

> licensees must exercise special care before using material relating to a child's personal or private affairs in the broadcast of a report of a sensitive matter concerning the child. The consent of a parent or guardian should be obtained before naming or visually identifying a child in a report on a criminal matter involving a child or a member of a child's immediate family, or a report which discloses sensitive information concerning the health and welfare of a child, unless there are exceptional circumstances or an identifiable public interest reason not to do so.

60.177 Two cases in New Zealand in 1999 heightened awareness of the privacy issues involved in filming and broadcasting of children.[231] Both of these cases involved filming and broadcasting of a child with parental permission, although in circumstances many people considered to be inappropriate. The cases led the Broadcasting Standards Authority of New Zealand to amend the privacy principles that are imposed on broadcasters in that country to include an additional privacy principle relating especially to children.[232] A reworded principle similar to that inserted in 1999 still exists in the 2006 version of the principles, with an additional principle that defines 'child'.

> Children's vulnerability must be a prime concern to broadcasters, even when informed consent has been obtained. Where a broadcast breaches a child's privacy, broadcasters shall satisfy themselves that the broadcast is in the child's best interests, regardless of whether consent has been obtained.
>
> For the purpose of these Principles only, a 'child' is defined as someone under the age of 16 years. An individual aged 16 years or over can consent to broadcasts that would otherwise breach their privacy.[233]

60.178 In a 1984 statement on identifying and interviewing children, then Federal President of the Australian Journalists' Association, John Lawrence, concluded that children under 12 should not be interviewed in circumstances where the adults caring

---

229 Although the ACMA *Privacy Guidelines for Broadcasters* (2005) make reference to the *Commercial Television Industry Code of Practice* and reproduce in appendices relevant sections from that Code relating to children.

230 *Commercial Television Industry Code of Practice* (2004) s 4.3.5.2.

231 One case involved a television broadcast of an eight year old boy with Attention Deficit Disorder (ADD) who clearly did not want to be filmed and the problems his mother faced trying to look after him. In the other case, a television broadcast showed a six year old boy, together with his parents, finding out who his father was after a paternity test. See M des Tombe, '"Get that Camera Out of My Face!" A Look at Children, Privacy and the Broadcasting Standards' (2000) 31 *Victoria University of Wellington Law Review* 577; K Ridley, 'Children and the Broadcasting Media: Respect for the Integrity and Rights of the Child?' (2000) 15(May) *Social Work Now* 6.

232 T McBride, 'Recent New Zealand Case Law on Privacy: Part II—The Broadcasting Standards Authority, the Media and Employment' (2000) 6 *Privacy Law & Policy Reporter* 133, 137.

233 New Zealand Government Broadcasting Standards Authority, *Privacy Principles* (2006).

for them are under stress.[234] This approach has not been incorporated into any guidelines issued within the industry.

Submissions and consultations

60.179 With the exception of the treatment of individuals accused of or charged with criminal offences, few submissions touched on the way in which the media use the personal information of children and young people.[235] Some examples were given of cases where a breach of privacy of a young person had been found, but there were minimal consequences for the media organisations involved.[236]

60.180 The New South Wales Commission for Children and Young People suggested that the existing media exemption does not protect adequately the privacy rights of children and young people, and that there should be a legislative requirement that broadcasters include, within their industry privacy standards, a standard that relates to children and young people specifically.[237] It considered that the standard should require broadcasters to consider the best interests of the child or young person, even where informed consent has been obtained from the child or his or her parent. This approach was considered to balance the desire of the industry to set its own standards, while sending a clear message about the industry's responsibilities to children and young people.[238] The New South Wales Commission for Children and Young People also supported OPC involvement in considering the adequacy of the industry standards. The Queensland Commission for Children and Young People and Child Guardian is currently developing guidelines for responsible portrayal of children in the media.[239]

ALRC's view

60.181 As noted in Chapter 38, submissions and consultations generally indicated that the exemption of media from the *Privacy Act* is necessary to provide for the free flow of information to the public. The exemption must be balanced, however, by providing an alternative mechanism to ensure adequate safeguards for the handling of personal information. Given the absence of extensive complaints about current media practices, the ALRC supports the retention of the media exemption. This should remain subject to the requirement that a media organisation observe privacy standards published by the organisation or a person or body representing a class of media organisations.

---

234 S Castell-McGregor, 'Children's Rights and the Media' (1985) 37 *Media Information Australia* 52, 53.
235 Issues relating to identification of individuals in relation to criminal matters are dealt with below.
236 Youth Issues Roundtable, *Consultation*, Melbourne, 7 February 2007.
237 NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.
238 Ibid.
239 Queensland Government Commission for Children and Young People and Child Guardian, *Submission PR 171,* 5 February 2007.

60.182 The ALRC sees a need, however, to improve the quality of media privacy standards, which at present impose varying privacy requirements and are lacking in detail. The ALRC proposes, therefore, that the OPC, in consultation with ACMA and peak media representative bodies, establish criteria for assessing the adequacy of media privacy standards.[240]

60.183 Given the particular vulnerabilities of children and young people, the ALRC considers that the privacy of children and young people should be addressed in media privacy standards. The ALRC proposes, therefore, that the criteria for assessing the adequacy of media privacy standards include consideration of the privacy of children and young people.

60.184 The ALRC has considered the possibility of requiring media organisations to obtain consent from a person with parental responsibility for the child or young person under a certain age before identifying or otherwise publishing personal information about the child or young person. Thought has also been given to imposing an additional obligation on media organisations to consider the best interests of the child or young person, even where parental consent is obtained.

60.185 Given the ALRC's approach to the media exemption in general, it is the preliminary view of the ALRC that it is not appropriate to impose particular obligations on media organisations in respect of children and young people. While concerns have been raised in submissions and consultations, they are not so extensive as to warrant legislative imposition of obligations inconsistent with the general media exemption. The ALRC considers that its proposals to improve the adequacy of privacy standards adhered to by media organisations, which will have to make specific reference to children and young people, are an appropriate response to the concerns raised. It is appropriate, however, that media organisations and bodies developing media privacy standards give consideration to issues regarding parental consent when handling the personal information of children and young people; and consider the best interests of the child or young person even where parental consent is obtained.

Proposal 60–8 The Office of the Privacy Commissioner should include consideration of the privacy of children and young people in the proposed criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

240 See Proposal 38–2. The ALRC also proposes clarification of the terms 'journalism' and 'publicly committed': Proposals 38–1, 38–3.

Identification in criminal matters and in court records

60.186 Information held by courts, including case files, judgments, and case management systems, often identify children and young people who are somehow associated with proceedings. They may be a party to a civil or administrative proceeding, a defendant or victim in a criminal matter, a child involved in a family law dispute, a witness, or merely mentioned as part of the proceedings.

60.187 The judicial records of courts are presently exempt from the *Privacy Act*.[241] Courts have traditionally been responsible for governing access to these records, and policies vary from court to court. As noted in Chapter 8, however, the advent of online access to court records opens up the possibility of these records being accessed easily by a large number of people for a variety of purposes. Given the extent of personal information that may be contained in court records, this raises significant privacy concerns.

60.188 The privacy of children and young people inside the court room has attracted more judicial and legislative protection than the privacy of children in other circumstances.[242] Both CROC and the Beijing Rules refer specifically to a young person's right to privacy at all stages of juvenile justice proceedings, whether accused or found guilty.[243] Rule 8.1 of the Beijing Rules notes that this is 'in order to avoid harm being caused to her or him by undue publicity or by the process of labelling'. The rule is explained in the official commentary.

> Young persons are particularly susceptible to stigmatization. Criminological research into labelling processes has provided evidence of the detrimental effects (of different kinds) resulting from the permanent identification of young persons as 'delinquent' or 'criminal'. Rule 8 also stresses the importance of protecting the juvenile from the adverse effects that may result from the publication in the mass media of information about the case (for example, the names of young offenders, alleged or convicted).[244]

60.189 Concerns also have been raised about the psychological damage that a child or young person involved in, or associated with, other kinds of cases might experience if identified in the media. This could include particularly difficult family law cases, child welfare cases, or high profile criminal law cases where the defendant has children who might suffer as a result of publication of the name or image of the accused.[245]

---

241 The ALRC does not propose to change this situation: see discussion in Ch 32.

242 J Moriarty, 'Children, Privacy and the Press' (1997) 9 *Child and Family Law Quarterly* 217, 219.

243 *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990), art 40(2)(b)(vii); *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8.1.

244 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8 commentary.

245 See, eg, R Taylor, 'Re S (A Child) (Identification: Restrictions of Publication) and A Local Authority v W: Children's Privacy and Press Freedom in Criminal Cases' (2006) 18 *Child and Family Law Quarterly* 269.

Stigma may attach to other cases such as immigration cases involving refusal of visas or applications for government payments.[246]

60.190 Based on the fundamental rule that proceedings take place in open court, the common law has developed principles regarding a court's power to suppress publication of certain details of evidence before the court, balancing certain public interests against the interests of open justice. One such public interest includes protecting the interests of children.[247] Many Australian courts and tribunals have specific powers to make suppression orders under their establishing legislation.[248]

60.191 Legislation relating to child welfare and criminal matters before children's courts in most jurisdictions have prohibitions on the publication of identifying information about a child who is involved in proceedings.[249] The *Family Law Act* has a more general prohibition in relation to any person who is a party, related to or associated with a party, or is a witness to proceedings.[250] The extent of the prohibitions vary, and in most cases the legislation permits, or a judge may permit, publication in certain circumstances.[251] One exception is the Northern Territory legislation relating to juvenile offenders, which has as its starting point that there is no prohibition on publication, but gives the court a discretion to order that a report, information relating to proceedings or the results of proceedings, not be publicised.[252]

Submissions and consultations

60.192 There was support for retaining the purpose-built provisions preventing the disclosure of the identity of a child or young person in relation to juvenile justice

---

246 For example, the case of *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83 involved a rejected application for Austudy at the student homeless rate, including addresses and details of the applicant's relationship with his parents. Note that *Migration Act 1958* (Cth) s 91X prohibits the publication of names of applicants for protection visas in the High Court of Australia, Federal Court of Australia or Federal Magistrates Court.

247 *Johnston v Cameron* (2002) 124 FCR 160, 167. It should be noted that in the United Kingdom, following the introduction of the *Human Rights Act 1998* (UK), much of the debate is now centred around competing rights such as the right to privacy versus the right to free speech: H Fenwick, 'Clashing Rights, the Welfare of the Child and the Human Rights Act' (2004) 67 *Modern Law Review* 889; I Cram, 'Minors' Privacy, Free Speech and the Courts' (1997) *Public Law* 410.

248 See, eg, *Federal Court of Australia Act 1976* (Cth) s 50; *Administrative Appeals Tribunal Act 1975* (Cth) s 35(2).

249 See, eg, *Children and Young Persons (Care and Protection) Act 1998* (NSW) s 105. The ALRC has recently recommended that federal sentencing legislation should prohibit the publication of a report of criminal proceedings involving a young person where the details would lead to, or be likely to lead to, the identification of the young person: Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), [27.62]–[27.66], Rec 27–1.

250 *Family Law Act 1975* (Cth) s 121.

251 See, eg, the power of the court to order that the name and identity of certain young convicted offenders be made public in *Juvenile Justice Act 1992* (Qld) s 234.

252 *Youth Justice Act 2005* (NT) s 50. See also discussion of a number of examples of media reporting in the Northern Territory in ABC Radio National, 'Naming and Shaming Juvenile Offenders', *Law Report*, 3 October 2006.

proceedings in the specific legislation in each jurisdiction.[253] The absence of such a provision in the Northern Territory, however, was seen as an area in need of reform.[254]

60.193 Some young people allegedly involved in criminal behaviour were named, or publicly identified through publication of their photograph, in the media following the Cronulla riots in December 2005.[255] It was suggested in a number of submissions that the provisions that restrict disclosure of the identity of children and young people should be extended to cover criminal investigations, as well as court proceedings, because the policy reasons for this protection apply at all stages of the criminal process.[256]

60.194 The ALRC did not receive any submissions suggesting there were problems with the handling of court records involving children and young people. Broader issues regarding privacy of court records are discussed in Chapters 8 and 32.

ALRC's view

60.195 In this Discussion Paper, and in a previous ALRC report,[257] the ALRC has noted the public policy reasons behind prohibiting the public identification of young people involved in criminal proceedings, in particular the rehabilitative aims of the juvenile justice system. It is of particular concern that the Northern Territory has no automatic limitation on publication of court proceedings that identify a young person. To protect the privacy of children and young people, the ALRC recommended in the report, *Same Crime, Same Time: Sentencing of Federal Offenders*, the enactment of a provision prohibiting the publication of a report of criminal proceedings that identifies, or is likely to lead to identification of, a child or young person.[258] The ALRC believes that such a prohibition remains appropriate, and is hopeful this recommendation will be implemented following government consideration of the entire report.

60.196 The ALRC also encourages consideration of broader provisions relating to public identification of a child or young person alleged to have committed a crime, applying throughout the criminal investigation and proceedings, whether in a court or alternative diversionary option. The ALRC considers that these kinds of provisions are situated most appropriately in relevant state and federal legislation dealing with child welfare or criminal matters. While related, this issue lies beyond the scope of this Inquiry and the ALRC has not made a proposal on the issue.

---

253 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

254 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

255 Ibid, NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007.

256 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007; Youthlaw, *Submission PR 152,* 30 January 2007; NSW Commission for Children and Young People, *Submission PR 120,* 15 January 2007.

257 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), [27.62]–[27.66].

258 Ibid, Rec 27–1. Due to the scope of the terms of reference of that inquiry, the recommendation was limited in application to the sentencing, administration and release of federal offenders.

Family law

60.197 Children and young people are often involved in counselling or family dispute resolution services undertaken as part of a family law dispute. Counselling and family dispute resolution services in association with family law disputes are now offered by private sector services (including not-for-profit services) which, unless they fall within an exemption, are subject to the NPPs.[259] The *Family Law Act 1975* (Cth) includes provisions governing the confidentiality of such services.[260] While an adult can give permission to have his or her information disclosed for any purpose, information provided by an individual under the age of 18 can be disclosed only with the agreement of each of the persons with parental responsibility for the child, or the approval of the court.[261] The exception that allows disclosure of information for research purposes specifically excludes the disclosure of personal information as defined in the *Privacy Act*.[262]

Submissions and consultations

60.198 Generally, submissions and consultations did not raise any issues of concern about the operation of the *Family Law Act* or the privacy policies in operation in the Family Court of Australia, Family Court of Western Australia or the Federal Magistrates Court.

60.199 The exception was the National Children's and Youth Law Centre, which indicated that the operation of ss 10D(3) and 10H(3) of the *Family Law Act*, which provide that information about a child may be disclosed if each of the persons with parental responsibility for the child agrees, operate contrary to the rights-based approach in the *Privacy Act* by excluding the involvement of the child in the decision-making process.[263]

ALRC's view

60.200 The ALRC agrees that ss 10D(3) and 10H(3) of the *Family Law Act* are not consistent with the proposed approach under the *Privacy Act* and the general principals of involvement of children and young people in decision making processes as set out in CROC. It would be appropriate to review these provisions, giving consideration to an improved process for involving a child or young person in the decision. The ALRC suggests that the Family Law Council would be the appropriate body to give further consideration to this issue.

---

259 Until 1 July 2006, confidential counselling and family dispute resolution services were also provided by specialised staff of the Family Court of Australia who are subject to the IPPs. These staff are now called 'family consultants' and no longer provide confidential services.

260 *Family Law Act 1975* (Cth) ss 10D, 10H. These provisions became operational on 1 July 2006.

261 Ibid ss 10D(3), 10H(3).

262 Ibid ss 10D(5), 10H(5).

263 National Children's and Youth Law Centre, *Submission PR 166,* 1 February 2007.

Child welfare and juvenile justice

60.201 Child welfare and juvenile justice jurisdictions are state and territory based. Children and young people who come into contact with either the child welfare or juvenile justice systems often have large amounts of personal information collected about them, much of it of a sensitive nature. Legislation in each jurisdiction deals with the handling of records in that jurisdiction containing personal information of children and young people.[264]

60.202 A privacy-related issue that has arisen in the area of child welfare is the sharing of information between agencies where the safety of children and young people is at issue. All states and territories have laws in place that, in practice, provide exceptions to privacy laws by allowing or requiring disclosure of personal information in certain circumstances. A number of bodies, however, have identified instances where a child has been seriously injured or killed by a parent where disclosure of information about the parent's behaviour to appropriate service providers could have helped to prevent the injury or death.[265]

60.203 The ALRC did not receive any submissions raising concerns about the handling of child welfare or juvenile justice records. However, issues surrounding the sharing of information in appropriate circumstances were raised as matters of concern.

ALRC's view

60.204 The issue of sharing information in child welfare and other contexts is considered in Chapter 11. The ALRC's proposed 'Use and Disclosure' principle, as discussed in Chapter 22, seeks to improve the balance between the need for information sharing in child protection while still maintaining an appropriate level of privacy protection. It is considered that the proposed changes to the existing disclosure principles, together with improved clarity of privacy laws generally and better information sharing practices, should alleviate many of the concerns raised in this context.

---

264 See, eg, *Children and Young Persons (Care and Protection) Act 1998* (NSW); *Juvenile Justice Act 1992* (Qld).

265 New South Wales Ombudsman, *Report of Reviewable Deaths in 2004* (2005); Child Death Review Team, *Fatal Assault of Children and Young People: Fact Sheet* (2003) New South Wales Commission for Children and Young People; Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

61. Adults with a Temporary or Permanent Incapacity

Contents

Introduction 1815
Equality and the presumption of capacity 1816
ALRC's view 1818
Problems with the *Privacy Act* 1819
Suggestions for reform 1822
Broader exceptions to the privacy principles 1822
An authorised representative mechanism 1825
Defining authorised representative 1826
Improved practices 1828
ALRC's view 1829
Changes to the proposed UPPs 1829
Adopting an authorised representative mechanism 1831
Defining authorised representative 1832
Limitations on liability of agencies and organisations 1834
Guidance and improved practices 1835

Introduction

61.1 This chapter considers existing laws and practices applying to the privacy of adults incapable of making decisions under the *Privacy Act 1988* (Cth). An incapacity may be temporary or permanent, and can be caused by many different circumstances, including disability, injury, illness or cognitive impairment.

61.2 There is a need to balance protecting this group of vulnerable individuals and ensuring that they are not marginalised or disadvantaged in accessing benefits and services. The ALRC proposes a number of new provisions for the *Privacy Act* to clarify rights and obligations when handling personal information about an individual incapable of making a decision under the Act, including by establishing and defining the term 'authorised representative' for a person able to make decisions on behalf of an incapable individual. The ALRC also proposes reforms aimed at facilitating practical implementation of these provisions for the benefit of incapable individuals and their authorised representatives.

61.3 This chapter focuses on circumstances in which an individual is incapable of making a decision, and a formal representative is required to make a decision on behalf of the individual. Chapter 62 deals with a broader range of circumstances where an individual requires assistance to make or communicate decisions under the Act, but does not require a substitute decision maker. This includes informal care arrangements as well as situations involving interpreters, counsellors and legal representatives.

61.4 Issues concerning sharing of information to improve the provision of services to vulnerable adults and others are dealt with in Chapter 11.

Equality and the presumption of capacity

61.5 This chapter deals with a range of circumstances in which an individual may be found to lack capacity to make a decision under the *Privacy Act*. In many cases, however, the individual will lack capacity because of a particular disability. Although an adult with a particular disability may not have the capacity to make decisions about how his or her personal information is handled, there is a need to ensure that his or her rights are protected.

> Personal information privacy is fundamental to a person's ability to enjoy their human dignity and autonomy. While everyone must compromise a reasonable level of their information privacy in order to live in society, people with decision-making disabilities are often expected to make far greater compromises than other people. Some compromises are reasonable so that a person can receive adequate services to meet their personal, health, financial or other needs and wishes. At the same time, people with decision-making disabilities are entitled to the same privacy rights as anyone else …[1]

61.6 In December 2006, the United Nations adopted the *Convention on the Rights of Persons with Disabilities*.[2] The Convention does not create new rights, but expresses existing rights in a manner that addresses the needs and situations of persons with disabilities.[3] Article 22 of the Convention deals with respect for the right of privacy.

> 1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.
>
> 2. State Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

---

1 Privacy NSW, *Best Practice Guide: Privacy and People with Decision-Making Disabilities* (2004), 2.

2 *Convention on the Rights of Persons with Disabilities*, 30 March 2007, UN Doc A/61/611 (not yet in force).

3 United Nations, *International Convention on the Rights of Persons with Disabilities: Why a Convention?* (2006) <www.un.org/disabilities/convention/about.shtml> at 1 August 2007.

61.7 The Australian Government participated in all negotiating sessions of the Convention's working group,[4] and was one of the first countries to sign the new Convention when it opened for signature on 30 March 2007.[5] If ratified by Australia, all legislation, policies and practices will need to be consistent with the new Convention.[6]

61.8 The New South Wales Disability Discrimination Legal Centre argued that the principle of autonomy of people with a disability is reflected in a range of international and domestic legal frameworks. It is not always easy to implement, however, as the person's capacity can change and alter over time and in relation to each issue.[7] The need for a case by case approach to determining capacity was stressed in a number of submissions.[8]

> Capacity is decision specific and impairment of decision-making capacity for some matters (that is, a person has impaired capacity for some types of financial or personal decisions and not others) only is typical. Adults with mental illness will typically have an episodic impairment of their capacity for decision-making. Even during periods when they are unwell, they will typically have capacity for decision-making about some types of matters but not others. Adults with acquired brain injury typically do not identify themselves as having a disability and often present well unless their plausibility is tested, but nevertheless they may have markedly impaired decision-making capacity as a result of gross impulsivity. Again, however, they may be able to make some types of decisions. Adults with dementia typically progress from early dementia, when they may retain or have fluctuating capacity for decision-making for many matters, but progressively become incapable of making decisions about matters.[9]

61.9 The concern is that some people may perceive automatically that an individual with a disability is incapable of making a decision under the *Privacy Act*. It may also be that some people will consider that an individual found to be incapable of making a decision at one point in time is incapable of making other decisions in the future. Legal Aid Queensland relayed its experience of individuals who, once it is disclosed that they have some form of intellectual disability, are required by certain organisations to produce a signed power of attorney or guardianship order and have all decisions made

---

4 Human Rights and Equal Opportunity Commission, 'Disability to Make UN Top Ten' (Press Release, 26 August 2006).

5 Australia did not sign the Optional Protocol to the Convention which deals with the competence of the Committee on the Rights of Persons with Disabilities to receive and consider communications from or on behalf of individuals or groups of individuals.

6 The Convention does not come into force until 30 days after the 20th instrument of ratification or accession is lodged. To date, 99 countries have signed but only one country has ratified the Convention.

7 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

8 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

9 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

by the authorised third party.[10] This approach is, in effect, discriminatory and undermines the privacy rights of the individual.

61.10 The *Disability Discrimination Act 1992* (Cth) provides broad protections against discrimination on the basis of an actual or perceived disability.[11] The Act's coverage extends to determining an individual's capacity to make a decision under the *Privacy Act*. If an individual considers he or she was treated unfairly by an agency or organisation because of his or her disability, a complaint can be made to the Human Rights and Equal Opportunity Commission under the *Disability Discrimination Act*.[12]

61.11 One approach that could be adopted is to specify clearly in the *Privacy Act* that there is a presumption that every individual aged 18 and over is capable of making a decision under the Act unless found to be incapable. This approach is adopted in guardianship and administration legislation in some jurisdictions.[13]

ALRC's view

61.12 The ALRC notes concerns about possible discrimination against people with a disability, and agrees that individuals aged 18 and over should be presumed to have capacity to make decisions under the *Privacy Act* unless found to be incapable of making that particular decision. The ALRC notes, however, that the fact that people with a disability are subjected to discrimination in relation to determining their capacity to make decisions under the Act was raised in only one submission to this Inquiry.

61.13 While agreeing with the application of the presumption in practice, the ALRC questions whether there is a need to set out the presumption in the *Privacy Act*. The ALRC proposes, below, that the Office of the Privacy Commissioner (OPC) develop and publish guidance for applying provisions relating to the determination of the capacity of individuals aged 18 and over.[14] Such guidance would note the possible fluctuating nature of the capacity of individuals, and the need to apply a presumption that an individual has capacity until found to not have capacity for a particular decision.

---

10 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

11 'Disability' is given a broad definition in the Act, encompassing physical, intellectual, psychiatric, sensory, neurological and learning disorders, illnesses, diseases, malfunctions or disabilities, as well as physical disfigurement and the presence in the body of disease-causing organisms: *Disability Discrimination Act 1992* (Cth) s 4.

12 Each state and territory also has anti-discrimination legislation and complaints bodies that cover discrimination on the basis of disability or impairment, although the detail of the laws differ: *Anti-Discrimination Act 1977* (NSW); *Equal Opportunity Act 1995* (Vic); *Anti-Discrimination Act 1991* (Qld); *Equal Opportunity Act 1984* (WA); *Equal Opportunity Act 1984* (SA); *Anti-Discrimination Act 1998* (Tas); *Discrimination Act 1991* (ACT); *Anti-Discrimination Act 1992* (NT).

13 See, eg, *Guardianship and Administration Act 2000* (Qld) sch 1, s 1.

14 Proposal 61–3.

61.14 The proposed guidance should set out how to make decisions in practice regarding capacity, and that the *Disability Discrimination Act* provides an appropriate mechanism for complaint if discrimination occurs. The ALRC is interested in further comment on whether there is a need for a legislative presumption, and whether there would be any adverse consequences of including such a presumption in the *Privacy Act*.

Question 61–1 Should the *Privacy Act* be amended to provide expressly that all individuals aged 18 and over are presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable of giving that consent, making that request or exercising that right?

Problems with the *Privacy Act*

61.15 General concerns were raised in submissions about the balance between protecting vulnerable adults from unnecessary interference with their privacy and ensuring that people gain access to required services and benefits.[15]

> The particular circumstances of people with a decision-making disability can mean that many aspects of their lives are unnecessarily exposed to others, and their privacy is compromised. However, it is important that protection of privacy does not have an undesired effect of creating further barriers to necessary service provision, which would result in poorer outcomes and reduced quality of life for the individuals concerned.[16]

61.16 The most significant issue raised in submissions is the need to ensure that privacy legislation enables appropriate third parties to act on behalf of others who cannot act for themselves. It was noted that there are inadequate alternative decision-making mechanisms in the *Privacy Act* to facilitate an exchange of information where an individual is unable to provide consent.[17] Examples were given of individuals experiencing difficulties in accessing a range of services or communicating with service providers because of real or perceived conflicts with the *Privacy Act*.[18] The most common concerns involved dealings with telecommunication corporations, utilities and financial institutions—organisations that individuals must deal with in

15 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007; Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

16 Government of South Australia, *Submission PR 187,* 12 February 2007.

17 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; National E-health Transition Authority, *Submission PR 145,* 29 January 2007.

18 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007; Australian Guardianship and Administration Committee, *Submission PR 129,* 17 January 2007; B Such, *Submission PR 71,* 2 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006; L Bennett, *Submission PR 21,* 11 June 2006; K Bottomley, *Submission PR 10,* 1 May 2006.

their everyday life for essential services. Problems arose when individuals attempted to make payments or defer payments on behalf of another individual, change account details, and access health information about adult relatives, particularly in relation to mental health. It was noted that it is often easy to enter into contracts or arrangements with organisations, but privacy concerns sometimes make it difficult to complain about a service or change service arrangements.[19] Similar concerns were raised in stakeholder forums conducted as part of the OPC review of the private sector provisions of the *Privacy Act* in 2005 (OPC Review).[20]

61.17 In 2003–04, the Australian Guardianship and Administration Committee (AGAC) undertook a small survey designed to determine whether there have been any unanticipated adverse consequences as a result of privacy legislation for people who have a decision-making disability. While finding that the legislation generally worked well, the AGAC concluded that there was 'significant room for improvement in how a range of service providers interpret and apply the legislation in cases involving people who have a decision-making disability and their family members and allies'.[21] The AGAC reiterated this view in a submission to this Inquiry.[22]

61.18 Most of the concerns raised by the AGAC related to inflexible interpretation and application of privacy legislation by frontline staff involved in providing services. The AGAC speculated that problems arise primarily because organisations, in an attempt to comply with the *Privacy Act*, require individuals expressly to authorise another person to transact business on their behalf.

61.19 The problems are most acute where there are informal arrangements in place for making decisions on behalf of an adult, such as where a family member, carer or friend makes decisions or assists in decision making. The existence of informal arrangements is consistent with the philosophy underpinning Australian guardianship and administration legislation. This legislation seeks to maximise involvement in decision making by the individual and ensure that the least restrictive decision-making processes are available. Formal guardianship or administration orders are made as a last resort where informal arrangements have broken down.[23] One view is that it would not be appropriate to require a formal guardian appointment merely to deal with privacy decisions because such an appointment places significant restrictions on the

---

19 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

20 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.

21 Australian Guardianship and Administration Committee, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

22 Australian Guardianship and Administration Committee, *Submission PR 129,* 17 January 2007.

23 Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Australian Guardianship and Administration Committee, *Submission PR 129,* 17 January 2007.

autonomy of the individual.[24] The Government of South Australia has particular concerns about individuals who do not have an active guardian.[25]

61.20 Concerns have been raised that, even in situations where a power of attorney or a formal guardianship or administration order is in place, these orders are not always respected.[26] There may be confusion about the information required before an organisation can be satisfied that an individual has consented to the disclosure to a third party of personal information.[27]

61.21 The New South Wales Disability Discrimination Legal Centre stated that the difficulties that have emerged in the implementation of privacy law for people with a decision-making disability have principally arisen because of three factors:

> first, the adoption of a narrow interpretation of the principle by utilities and service providers (such as water and electricity utilities, banks and insurance companies); second, a private and public sector culture at the level of 'front line workers' of 'risk minimisation' in approaching privacy laws; and third, the reliance on 'informal' arrangements in supported decision making, where a family member, friend, or carer acts as a supported substitute decision maker for a person with impaired decision making capacity without formal authorisation.[28]

61.22 A more specific concern was raised by the Office of the Public Advocate Victoria which noted problems concerning requirements to notify individuals if personal information is collected from someone other than the individual.[29] The Office noted that the requirement is problematic when dealing with an individual with a significant cognitive impairment. In some cases, people have had to be engaged especially to help explain the content of the notification to an individual. Apart from the added expense, this expands the number of people who have access to the personal information.

---

24 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007.

25 Government of South Australia, *Submission PR 187,* 12 February 2007.

26 K Bottomley, *Submission PR 10,* 1 May 2006. This concern was also identified by a number of callers to the ALRC National Privacy Phone-In.

27 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.

28 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

29 Office of the Public Advocate Victoria, *Submission PR 141,* 24 January 2007. At present, there is an onus on an organisation to take 'reasonable steps' to provide the notification, and the only exception to this requirement is where the notification would pose a serious threat to the life or health of any individual: *Privacy Act 1988* (Cth) sch 3, NPP 1.5.

Suggestions for reform

Broader exceptions to the privacy principles

61.23 As discussed in Chapter 60, the *Privacy Act* may require decisions to be made or actions to be taken by an individual at various points in the information-handling cycle. These include:

- consenting to the collection of sensitive information;[30]
- consenting to a particular use or disclosure of personal information, and in particular, consenting to use for the purposes of direct marketing;[31]
- consenting to the transfer of personal information outside of Australia;[32]
- requesting not to receive further direct marketing communications from an organisation;[33]
- requesting access to personal information held by an organisation;[34]
- opting for anonymity or pseudonymity in transacting with any agency or organisation;[35]
- making a complaint against an agency or organisation.[36]

61.24 In situations where consent of the individual is required, there are carefully crafted exceptions that allow an agency or organisation to undertake the action without consent. The OPC Review indicated that the 'authorised by law' exception in a number of the existing Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) enables the collection of sensitive information from, or disclosure of personal information to, a third party where a formal guardianship or administration order is in place.[37] These 'authorised by law' exceptions have been included in the ALRC's

30 See proposed 'Collection' principle and discussion in Ch 18.
31 See proposed 'Use and Disclosure' principle and 'Direct Marketing' principle and discussion in Chs 22 and 23.
32 See proposed 'Transborder Data Flows' principle and discussion in Ch 28.
33 See proposed 'Direct Marketing' principle and discussion in Ch 23.
34 See proposed 'Access and Correction' principle and discussion in Ch 26. It is proposed that access to personal information held by an agency should be governed by a new Part of the *Privacy Act 1988* (Cth): see Proposal 12–6.
35 See proposed 'Anonymity and Pseudonymity' principle and discussion in Ch 17.
36 See discussion in Ch 45.
37 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 214–215.

proposed Uniform Privacy Principles (UPPs).[38] The OPC Review also stated that a third party is able to exercise a right on behalf of an individual where a formal guardianship or administration order is in place, despite the absence of an express provision to that effect in the Act.[39]

61.25 Detailed provisions exist in relation to the disclosure of health information about persons incapable of giving consent. NPPs 2.4, 2.5 and 2.6 establish a scheme that facilitates, within certain limits, disclosure of health information to 'responsible' persons. The disclosure of health information is only permissible where the individual is incapable of providing consent, and the carer providing the health service is satisfied that either the disclosure is necessary to provide appropriate care or treatment, or the disclosure is to be made for compassionate reasons.[40] The disclosure must not be contrary to any wish expressed by the individual before they were incapacitated, and the disclosure must be limited to the extent reasonable and necessary for the purpose of disclosure.[41] 'Responsible' person is defined to include a:

- parent of the individual;
- child or sibling of the individual and at least 18 years old;
- spouse or de facto spouse of the individual;
- relative of the individual, at least 18 years old and a member of the individual's household;
- guardian of the individual;
- person exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;
- person who has an intimate personal relationship with the individual; and
- person nominated by the individual to be contacted in case of emergency.[42]

---

38 Note that the relevant exception in the proposed 'Collection' principle has been narrowed so that sensitive information can be collected without consent where 'required or *specifically* authorised by law': see Proposal 19–2.

39 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.

40 *Privacy Act 1988* (Cth) sch 3, NPP 2.4(a), (b).

41 Ibid sch 3, NPP 2.4(c), (d).

42 Ibid sch 3, NPP 2.5. The terms 'parent', 'child', 'relative' and 'sibling' are defined in NPP 2.6.

61.26 While the *Privacy Act* currently provides for agencies and organisations to deal with formal guardianship and carer arrangements, concerns about the implementation of existing provisions indicate the need for clearer provisions and improved practices. With the exception of disclosure of health information in limited circumstances, informal care arrangements are not recognised by the *Privacy Act* or in practice.

61.27 One option for reform, recommended by the OPC Review, is to amend the exceptions to the proposed UPPs to expand the circumstances in which a third party may provide consent on behalf of an incapable individual, or access information about that individual.[43] In particular, the OPC Review recommended amending the 'Use and Disclosure' NPP to permit a disclosure of non-health information in a similar way to disclosure of health information under NPP 2.4. As in NPP 2.4, the purpose and circumstances of the disclosure could be limited appropriately. The OPC Review suggested that disclosure should be permitted only where an organisation considers the disclosure necessary for the management of the affairs of an individual with decision-making disabilities, in a way that his or her financial or other interests are safeguarded.[44]

61.28 There is a question as to whether exceptions to other UPPs, in particular the proposed 'Sensitive Information' principle, should be expanded to facilitate better decision making by a substitute decision maker where an individual is incapable of making a decision under the *Privacy Act*.

61.29 There was some support in submissions for extending the exception in NPP 2.4 to other personal information.[45] The New South Wales Guardianship Tribunal considered that the provisions in NPP 2.4 are too restrictive and place too great an onus on the person providing the health service to make an assessment about a number of potentially difficult matters before disclosure can be made.[46] The Tribunal did, nevertheless, support extension of this kind of approach to non-health information.

61.30 On the other hand, the New South Wales Disability Discrimination Legal Centre opposed extending the exception to other personal information.[47] While acknowledging the problems faced by informal representatives, the Centre considered that the solution should not be achieved through dilution of the protections of the *Privacy Act*, which might leave a vulnerable person open to abuse, in particular, financial abuse. The Office of the Public Advocate Queensland submitted that the threat of abuse is real, and pointed to research estimating that 4.6% of older people experience physical, sexual or financial abuse. It is thought that, in most cases, the perpetrators of abuse are

---

43 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 63.

44 Ibid, rec 63.

45 Queensland Council for Civil Liberties, *Submission PR 150,* 29 January 2007; Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.

46 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007.

47 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

family members or someone who is in a duty of care relationship with the older person.[48]

61.31 While generally not supporting the OPC Review's recommendation, the New South Wales Disability Discrimination Legal Centre made suggestions about how any extension of the disclosure exception to non-health personal information might be restricted.[49] The Centre suggested that, to be permissible, the disclosure should be reasonable, related to an authorised purpose, and derogate from the individual's right to privacy as little as a reasonable person would consider acceptable. The Council of Social Service of New South Wales similarly noted that it is 'imperative that the information accessed or made available to the guardian/carer must only be information that contributes or assists in the management of the present situation'.[50]

An authorised representative mechanism

61.32 An alternative approach is to establish separate provisions in the *Privacy Act* that acknowledge a process for substitute decision makers. This kind of approach is adopted in the *Health Records and Information Privacy Act 2002* (NSW), the *Health Records Act 2001* (Vic) and the draft *National Health Privacy Code*. While some of the details differ, each of the Acts and the Code have separate provisions that:

- provide guidance on determining the capacity of an individual;
- establish that an authorised representative may act and make decisions on behalf of an individual who does not have capacity; and
- define who may act as an authorised representative.[51]

61.33 A similar mechanism in the *Privacy Act* would avoid the need to craft specific exceptions in the proposed UPPs to cover authorised representatives and substitute decision making. The provisions relating to determination of capacity would provide greater clarity for agencies and organisations making these assessments. A number of stakeholders supported the 'authorised representative' and determination of capacity provisions in the New South Wales and Victorian Acts and the draft *National Health Privacy Code*.[52]

---

48 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007, citing R Munro, 'Elder Abuse and Legislative Remedies: Practical Remedies' (2002) 81 *Reform* 42.

49 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

50 Council of Social Service of New South Wales, *Submission PR 115,* 15 January 2007.

51 *Health Records and Information Privacy Act 2002* (NSW) ss 7–8; *Health Records Act 2001* (Vic) s 85; National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4 cls 1, 4.

52 New South Wales Guardianship Tribunal, *Submission PR 209,* 23 February 2007; Australian Nursing Federation, *Submission PR 205,* 22 February 2007; Office of the Health Services Commissioner

Defining authorised representative

61.34 The draft *National Health Privacy Code* defines an authorised representative as a person who is:

> (a) a guardian of the individual appointed under law; or
>
> (b) an attorney for the individual under an enduring power of attorney; or
>
> (c) a person who has parental responsibility for an individual who is a child; or
>
> (d) otherwise empowered under law to perform any functions or duties as an agent or in the best interests of the individual—
>
> except to the extent that acting as an authorised representative of the individual is inconsistent with an order made by a court or tribunal.[53]

61.35 In relation to adults, this list is fairly narrow and reflects a level of formality in appointing or empowering the third party to act as an authorised representative.

61.36 As noted above, some stakeholders urged that the need to reduce barriers for vulnerable adults and their carers justified acknowledging a broad category of people able to act on behalf of others without capacity. The Office of the Public Advocate Queensland supported recognition of substitute decision makers who are not formally appointed, but suggested more stringent requirements where serious consequences may flow from disclosure of personal information.[54] This would apply both to the requirements to determine if a person has capacity, and the identification and authorisation of the substitute decision maker. For example, the Office suggested more stringent identification requirements for financial matters, where there is a greater risk of abuse, and a limit of $5,000 on the amount of the financial transaction.

61.37 In the health area, while there was overall support for the authorised representative mechanism used in the *Health Records Act* and draft *National Health Privacy Code*, some were concerned about the existing definition. The National E-health Transition Authority (NEHTA) considered the definition too narrow.

> Through NEHTA's consultation activities, it is clear that health consumers and healthcare providers alike seek sufficient flexibility in privacy law to allow the right person to stand in for another to make decisions, when appropriate, about the handling

---

(Victoria), *Submission PR 153,* 30 January 2007; National E-health Transition Authority, *Submission PR 145,* 29 January 2007; Office of the Public Advocate Victoria, *Submission PR 141,* 24 January 2007; Department of Health Western Australia, *Submission PR 139,* 23 January 2006; Australian Government Department of Human Services, *Submission PR 136,* 19 January 2007; Centre for Law and Genetics, *Submission PR 127,* 16 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

53 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4 cl 1. The definitions in the *Health Records and Information Privacy Act 2002* (NSW) and *Health Records Act 2001* (Vic) are very similar, although these Acts make specific reference to particular state legislation relating to guardianship and administration and, in Victoria, agents acting within the meaning of the *Medical Treatment Act 1988* (Vic).

54 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

> of their personal and health information. Such flexibility must be balanced against an organisation's need for confidence (and management of liability risk), requiring the person acting for the individual concerned to have verifiable authority to act. Professional judgement exercised by a healthcare provider is generally considered to be a valuable decision-making tool, able to take account of the specific facts and circumstances at hand.[55]

61.38 The Office of the Health Services Commissioner (Victoria) suggested incorporating the definition of 'person responsible' as set out in the *Guardianship and Administration Act 1986* (Vic), which includes a hierarchy of specific persons such as unpaid primary carers and relatives but gives greater certainty than a broad 'catch all' provision.[56]

61.39 The Australian Bankers' Association (ABA) was concerned about being able to recognise appropriate substitute decision makers. While acknowledging that an enduring power of attorney is likely to suffice in most circumstances, subject to appropriate identification checks, the ABA considered it would be safer 'for all concerned' if an order or authority were obtained under guardian and administration legislation for the purposes of the *Privacy Act*.[57] There is evidence to suggest that enduring powers of attorney are often a catalyst for a significant amount of financial abuse.[58] The ABA noted that its members are also bound by the bankers' duty of confidentiality.

> While supporting flexibility and maintaining reasonable informality for these agency relationships is needed to be effective, there is a unique issue for banks due to the banker's duty of confidentiality. To comply with this duty a bank must be satisfied that an agent is duly authorised to act for the principal before the bank can disclose details of the customer relationship to the agent. Express authorisation is often required from the customer … The central issue here is not the practical difficulties of such persons accessing and engaging in banking transactions and services but having in place an adequate level of protection to prevent financial abuse and criminal behaviour to the detriment of the customer.[59]

61.40 The ABA stated that it would consider processes involving greater informality in authorising substitute decision makers if organisations were provided with appropriate protections against liability.[60]

---

55 National E-health Transition Authority, *Submission PR 145,* 29 January 2007.

56 Office of the Health Services Commissioner (Victoria), *Submission PR 153,* 30 January 2007. The definition of 'person responsible' set out in the *Guardianship and Administration Act 1986* (Vic) s 37 is adopted and incorporated into the *Health Records Act 2001* (Vic) s 85(6)(d).

57 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

58 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

59 Australian Bankers' Association Inc, *Submission PR 259,* 19 March 2007.

60 Ibid.

61.41 Achieving an appropriate balance between privacy protection and facilitating transactions is not easy. As noted by the Office of the Public Advocate Queensland:

> The task of appropriately providing a privacy regime which supports the adults where the substitute decision-maker seeks to act informally is far from straight-forward. Desirably, information should be made available to the substitute decision-maker when this is appropriate, but not, when it is not. This seems obvious, but the practicality of designing an appropriate scheme and its implementation are both problematic.[61]

Improved practices

61.42 The experiences and frustrations of individuals indicate that there are inconsistent practices in place in agencies and organisations, and in some cases practices that are not necessarily in accordance with the *Privacy Act*.

> It seems to me that many businesses hide behind the Act so that they do not have to do anything about the request being made to them and so just refuse point blank to even listen or make any attempt to try to solve the dilemma that you find yourself in. People should be treated with dignity at all times and should not be intimidated and belittled. Both the person who is making the request and the person from whom the request came should be respected and treated as a human being and not as a nuisance and a hindrance to the running of the business.[62]

61.43 To meet the needs of its clients better, Centrelink has adopted a nominee arrangement which allows individuals to nominate a third party to do the following on behalf of the individual:

- make enquiries only (person permitted to enquire);
- receive payments (payment nominee); or
- act and make changes generally (correspondence nominee).[63]

61.44 Nominee arrangements can be voluntary, and authorise any person to be the nominee with the consent of the individual. These arrangements are also used by Centrelink to recognise formal care relationships including powers of attorney, court or tribunal orders, and guardianship and administration orders. Each type of nominee has a different level of responsibility, and payment and correspondence nominees have an obligation to act in the best interests of the individual he or she represents.

---

61 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

62 K Bottomley, *Submission PR 10,* 1 May 2006.

63 The same person or organisation may be authorised as both a payment and correspondence nominee, or two different people or organisations may be authorised as separate nominees.

61.45 Centrelink's nominee arrangements are underpinned by legislation,[64] but it has been suggested that similar arrangements could operate administratively, as the Centrelink arrangements have in the past.[65] The Office of the Public Advocate Queensland noted that without the operation of the nominee arrangement at Centrelink, many people with an impaired capacity would not have received benefits to which they were entitled.[66] Centrelink's nominee arrangements have recently been revised to clarify the role and strengthen the accountability of the nominee, and to allow for removal of the nominee in appropriate circumstances.[67] A number of other agencies and organisations have adopted some version of a nominee arrangement.[68]

61.46 The OPC Review recommended the creation of more guidance to assist in the development of appropriate decision-making practices consistent with the law. In particular, it pointed to the best practice documentation in relation to people with decision-making disabilities developed by Privacy NSW.[69] The need for detailed guidelines to improve awareness of the law and provide guidance on assessing capacity and recognising legitimate relationships between individuals with an incapacity and their carers was highlighted in a number of submissions.[70]

ALRC's view

Changes to the proposed UPPs

61.47 The ALRC does not consider it appropriate to provide for substitute decision making through exceptions in the proposed UPPs. The ALRC has adopted the approach of developing high level principles that are flexible and adaptable to the multitude of circumstances in which agencies and organisations must take account of individuals' privacy rights. The principles are also resilient to change.[71] Any exceptions contained in the UPPs will have broad application. While it is possible to develop particular exceptions to rectify some of the issues concerning individuals

---

64 *Social Security (Administration) Act 1999* (Cth) pt 3A, which was inserted by the *Family and Community Services Legislation Amendment (Budget Initiatives and Other Measures) Act 2002* (Cth).

65 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

66 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

67 Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

68 Nominee arrangements are discussed in detail in Ch 62.

69 Privacy NSW, *Best Practice Guide: Privacy and People with Decision-Making Disabilities* (2004). This documentation was developed for New South Wales public sector agencies handling personal information in accordance with the *Privacy and Personal Information Protection Act 1998* (NSW).

70 Legal Aid Queensland, *Submission PR 212,* 27 February 2007; Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007; Legal Aid Commission of New South Wales, *Submission PR 107,* 15 January 2007; NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.

71 The ALRC's general approach to the development of the proposed UPPs is discussed in Ch 15.

without capacity, their general application could have unforeseen consequences. To avoid this, the exceptions would need to be drafted with a level of detail the ALRC is generally trying to avoid in the proposed UPPs.

61.48 The ALRC proposes, therefore, that mechanisms for dealing with authorised representatives should be set out in separate provisions in the *Privacy Act* and have application across all of the proposed UPPs and other provisions of the Act.

61.49 The ALRC has, however, given careful consideration to the needs of individuals with limited or no capacity when developing each of the proposed UPPs. In particular, the exceptions to consent set out in the proposed 'Sensitive Information' and 'Use and Disclosure' principles must have regard to circumstances where consent cannot be obtained from the individual or an authorised representative. In Chapter 19, the ALRC asks whether there is a need to expand the circumstances in which sensitive information can be collected without the consent of the individual to include situations that involve provision of an essential service for the benefit of the individual.[72]

61.50 It also may be appropriate to provide for particular circumstances in which certain types of personal information can be collected or disclosed without the consent of the individual. The ALRC considers that the existing provisions of NPPs 2.4 and 2.5 provide an appropriate exception in relation to disclosure of health information to the widely defined 'responsible' person in the limited circumstances provided. The ALRC proposes, therefore, to incorporate this exception into the proposed *Privacy (Health Information) Regulations*, which will apply only to health information.[73]

Specific notification

61.51 The ALRC notes the concerns expressed by the Office of the Public Advocate Victoria regarding notification requirements where the individual involved has a significant cognitive impairment. The ALRC has given careful consideration to the notification requirements, and has proposed a number of amendments to the existing NPP 1.5 to be incorporated into the proposed 'Specific Notification' principle.[74] In particular, the requirement will only apply in circumstances where a reasonable person would expect to be notified.[75] The existing exception, that notification is not required where this would pose a serious threat to the life or health of any individual, has been retained.

61.52 Beyond these exceptions, the ALRC considers it is appropriate to take steps to explain the notification to individuals with a cognitive impairment. The notification requirement exists as an important mechanism for an individual to retain some control

---

72 Question 19–1.

73 See discussion of the proposed *Privacy (Health Information) Regulations* and their intended operation in Chs 56, 57.

74 The principle and its application are discussed in Ch 20.

75 Proposal 20–5.

over the quality of personal information about them. The requirement to take steps to explain the notification is consistent with the proposal in this chapter that requires agencies and organisations to provide assistance to individuals to understand and communicate decisions that must be made under the *Privacy Act*. There will be circumstances in which it is acceptable to involve a third party to assist individuals to understand their rights and responsibilities under the Act, even where this may result in disclosure to a third party of personal information about the individual.[76]

61.53 Where the cognitive impairment is so severe that the individual will not be able to understand the notification even with assistance, it would be consistent with the proposed 'Specific Notification' principle and the proposals in this chapter to provide notification to the authorised representative if one exists. Guidance on this issue could be set out in the proposed guidance on the handling of personal information about individuals with a temporary or permanent incapacity.[77]

Adopting an authorised representative mechanism

61.54 The ALRC proposes that the *Privacy Act* should be amended to incorporate provisions that define the concept and role of authorised representatives in decision making. The ALRC considers that the *Health Records Act* and the draft *National Health Privacy Code* should be used as a model.[78]

61.55 The first step is to establish the circumstances in which an authorised representative is required or authorised to make a decision on behalf of an individual. The ALRC considers that an authorised representative should only be able to make a decision on behalf of an individual where the individual has been assessed as incapable of making the particular decision.[79] At present, the *Privacy Act* does not provide any guidance on what it means to have capacity. The ALRC proposes the introduction of a provision similar to s 85(3) of the *Health Records Act*, which reads:

> For the purposes of sub-sections (1) and (2), an individual is incapable of giving consent, making the request or exercising the right of access if he or she is incapable by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of—
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or

---

76 See discussion about involvement of third parties with the consent of the individual in Ch 62.

77 See Proposal 61–3 below.

78 The *Health Records and Information Privacy Act 2002* (NSW) provisions have similar operation, but are set out slightly differently. The ALRC proposals are based more closely on the provisions in the *Health Records Act 2001* (Vic) and the draft *National Health Privacy Code*.

79 It is not intended that the concept of authorised representative be applied to a deceased individual: see Ch 3.

> (b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires)—
>
> despite the provision of reasonable assistance by another person.[80]

61.56 The ALRC considers that the term 'senility' should be replaced with 'cognitive impairment', which covers a wider range of impairments and includes senility. The ALRC also considers that the descriptive list is not intended to be finite, and suggests that the words 'or any other circumstance' should be included to cover any circumstance that has led to a temporary or permanent incapacity.

61.57 In Chapter 60 the ALRC proposes to adopt the same test for determining incapacity of an individual under the age of 18. In that case, the term 'maturity' also should be incorporated into the list of circumstances that may be the basis of the incapacity.

61.58 The ALRC considers that the requirement to provide reasonable assistance to the individual to understand and communicate his or her decision is an important component of the proposed provision. Direction on what is considered to be 'reasonable assistance' should be included in the proposed guidance, to be developed by the OPC, on applying the provisions relating to adults with a temporary or permanent incapacity.[81]

Defining authorised representative

61.59 There are conflicting views on who the *Privacy Act* should recognise as an authorised representative. On the one hand, there is a need for flexibility so as not to disenfranchise adults who may have an impaired capacity or other disability that makes it difficult for them to communicate directly with agencies and organisations. On the other, it is important to ensure that the privacy of vulnerable adults is given appropriate protection. As access to personal information about an individual can also expose the individual to risk of financial or other abuse, it is important to ensure the right balance is provided in the *Privacy Act*.

61.60 The concept of the authorised representative is only intended to operate where an individual is found to be lacking the capacity to make a particular decision under the *Privacy Act*. It is the preliminary view of the ALRC that a broad definition of authorised representative would dilute the protections provided by the *Privacy Act*. There must be an appropriate framework for determining who can act on behalf of an individual incapable of making a decision in his or her own right.

61.61 The ALRC proposes to introduce a definition of authorised representative based on that in the draft *National Health Privacy Code*. This Code was developed to have

---

80 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4 cl 4(3) is identical.

81 See Proposal 61–3 below.

national coverage, and makes no reference to specific legislation, but is similar to the legislation operating in New South Wales and Victoria. The ALRC considers that the definition appropriately covers the categories of persons that should be recognised as an authorised representative for the purposes of the *Privacy Act*, with one exception—the term 'enduring guardian' should be added to the list to capture the full range of appointments available in each state and territory. A number of states provide for the appointment of an enduring guardian, rather than an enduring power of attorney, to make decisions in relation to medical or lifestyle matters.[82] A provision should also be incorporated into the *Privacy Act* to clarify that an authorised representative is not to act in any way that is inconsistent with an order made by a court or tribunal, in contravention of the terms of any appointment under law, or beyond the powers provided for in an enduring power of attorney.

61.62 The ALRC proposes the retention of provisions, based on those in NPPs 2.4 and 2.5, which allow for disclosure of health information in specific situations where the individual is unable to provide consent.[83] 'Responsible' person is broadly defined, and the ALRC considers this appropriate in relation to disclosure of health information where emergency situations are common and linked to decisions regarding medical treatment.

61.63 The ALRC is also attracted to the operation of nominee arrangements in place in a number of agencies and organisations. The ALRC considers that appropriate acknowledgement and implementation of such arrangements would prove beneficial for informal care arrangements where the individual has full, partial, or intermittent capacity. Nominee arrangements are considered in detail in Chapter 62.

61.64 It may also be appropriate to incorporate the concept of a nominee into the definition of authorised representative to cover situations where individuals know they have an intermittent capacity, or are entering a situation where they know they will lose capacity temporarily or permanently—such as prior to surgery or the onset of a debilitating illness. It may be appropriate in such circumstances to recognise a person who was nominated by the individual at a time when he or she had capacity. This would provide flexibility and control for the individual to choose his or her own representative without the need for formal appointment. Some process would, however, be required to inform the relevant agency or organisation of the nomination, and ensure that the individual had the true capacity to make the nomination at the time.

---

82 See, eg, *Guardianship Act 1987* (NSW) pt 2; *Guardianship and Administration Act 1993* (SA) pt 3; *Guardianship and Administration Act 1995* (Tas) s 32. A good overview of the various types of power of attorney by state and territory is provided in Credit Union Services Corporation, *Powers of Attorney: Making Your Own Decisions* (2002), 5.

83 See Ch 57.

61.65 It could be argued that state and territory legislation that provides for the appointment of an enduring power of attorney or an enduring guardian already fulfils the purpose of nominating a person prior to the loss of capacity. The state and territory legislation establishes proper processes for making such an appointment and imposes appropriate obligations on the appointed attorney or guardian. As enduring powers of attorney and enduring guardians are already recognised in the proposed definition of 'authorised representative', it is open for discussion whether a less formal nomination mechanism should be recognised. The ALRC is seeking further input on this question.

Limitations on liability of agencies and organisations

61.66 If agencies and organisations do not give appropriate recognition to authorised representatives of individuals incapable of making decisions under the *Privacy Act*, the privacy of these individuals may be compromised, and their access to essential services and benefits may be affected. Agencies and organisations must, however, take steps to ensure that only appropriate third parties have access to personal information about individuals. The guidance and training initiatives proposed below should help agencies and organisations to meet their obligations.

61.67 The ALRC is conscious of the responsibility imposed on agencies and organisations by the authorised representative mechanism. As under some other legislation, the ALRC considers it appropriate to set some limits on the responsibilities of agencies and organisations when dealing with authorised representatives.

61.68 Agencies and organisations should be required to take reasonable steps to validate the authority of an authorised representative. Guidance should set out what are considered to be reasonable steps. The Office of the Public Advocate Queensland suggested that a certified copy of the document or order should be produced, together with a statutory declaration confirming that the appointee is not aware of any subsequent appointment.[84] The agency or organisation should check to ensure that the decision or action being taken by the authorised representative falls within the authority of the document or order.

61.69 Where reasonable steps are taken, the ALRC does not consider that agencies and organisations should be responsible for relying on the decision or action of the authorised representative if it is later found that the authorised representative was not properly appointed, or exceeded the authority of his or her appointment. In these circumstances, the agency or organisation should not be considered to have engaged in conduct constituting an interference with the privacy of an individual under the *Privacy Act*.

84 Office of the Public Advocate Queensland, *Submission PR 195,* 12 February 2007.

Guidance and improved practices

61.70 Many submissions pointed to inconsistent and improper practices of agencies and organisations handling personal information about individuals with an impaired capacity, or communicating with these individuals and their representatives. While the ALRC's proposals should help to clarify the obligations of agencies and organisations, there will be a need to ensure that they are aware and understand the operation of the provisions. The ALRC proposes, therefore, a number of practical measures to raise the level of awareness and improve the application of the provisions in practice. These proposals are similar to proposals made in Chapter 60 in relation to the handling of personal information about individuals under the age of 18.

61.71 The ALRC proposes that the OPC develop and publish guidance for agencies and organisations concerning the handling of personal information about individuals with a temporary or permanent incapacity. Much of the guidance will be about the appropriate way to communicate with individuals and their representatives. This should include guidance on the responsibility to provide reasonable assistance to individuals to assist them to understand and communicate decisions under the *Privacy Act*, enhancing their capacity to make decisions. Guidance on applying the criteria for determining an individual's capacity would also be useful to agencies and organisations. Guidance should also deal with what are considered to be 'reasonable steps' in determining the authority of a person to act as an authorised representative.

61.72 In Chapter 21, the ALRC proposes that all agencies and organisations subject to the *Privacy Act* develop and publish a Privacy Policy that sets out how the agency or organisation manages personal information and how personal information is collected, held, used and disclosed.[85] Agencies and organisations that handle personal information about adults incapable of making decisions under the Act should address in their Privacy Policies how such information is managed. This would include addressing issues such as the requirement to communicate with authorised representatives where an individual is found to be incapable, and how to identify authorised representatives.

61.73 The ALRC also considers that agencies and organisations that regularly handle personal information about individuals with a temporary or permanent incapacity should ensure that their staff are trained adequately to assess the capacity of individuals. Staff should be made aware of the steps to be taken to identify an authorised representative, and how to communicate appropriately with the individual and the authorised representative. Training should also encompass any nominee arrangements established by the agency or organisation.[86] It may be appropriate that such training is offered by industry associations, possibly as part of broader training

85 See Proposals 21–1, 21–2, 21–3, 21–4.

86 See the discussion of nominee arrangements in Ch 62.

programs aimed at improving staff awareness and practices in relation to personal information.

Proposal 61–1 The *Privacy Act* should be amended to provide that an individual aged 18 or over is incapable of giving consent, making a request or exercising a right under the Act if, despite the provision of reasonable assistance by another person, he or she is incapable by reason of injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability, or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

(b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.

Where an individual is considered incapable of giving consent, making a request or exercising a right under the Act, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of the individual.

Proposal 61–2 The *Privacy Act* should be amended to introduce the concept of 'authorised representative', defined as a person who is, in relation to an individual:

(a) a guardian of the individual appointed under law;

(b) a guardian for the individual under an appointment of enduring guardianship;

(c) an attorney for the individual under an enduring power of attorney;

(d) person who has parental responsibility for the individual if the individual is under the age of 18; or

(e) otherwise empowered under law to perform any functions or duties as agent or in the best interests of the individual.

The *Privacy Act* should state that an authorised representative is not to act on behalf of the individual in any way that is inconsistent with an order made by a court or tribunal, in contravention of the terms of any appointment under law, or beyond the powers provided for in an enduring power of attorney.

Question 61–2 Should the definition of 'authorised representative' include a person who was nominated by the individual at a time when the individual had the capacity to make the nomination?

Proposal 61–3 The *Privacy Act* should be amended to provide that an agency or organisation that has taken reasonable steps to validate the authority of an authorised representative will not be considered to have engaged in conduct constituting an interference with privacy of an individual merely because it acted upon the consent, request or exercise of a right by that authorised representative, if it is later found that the authorised representative:

(a) was not properly appointed; or

(b) exceeded the authority of his or her appointment.

Proposal 61–4 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals aged 18 and over incapable of giving consent, making a request or exercising a right on their own behalf, including on:

(a) the provision of reasonable assistance to individuals to understand and communicate decisions; and

(b) practices and criteria to be used in determining whether an individual is incapable of giving consent, making a request or exercising a right on his or her own behalf.

Proposal 61–5 Agencies and organisations that handle personal information about people incapable of making a decision should address in their Privacy Policies how such information is managed.

Proposal 61–6 Agencies and organisations that regularly handle personal information about adults incapable of making a decision should ensure that their staff are trained adequately to assess the decision-making capacity of individuals.

62. Other Third Party Assistance

Contents

Introduction	1839
Problems with the *Privacy Act* in practice	1839
Existing third party arrangements	1841
ALRC's view	1844

Introduction

62.1 This chapter considers practices allowing third parties to assist or act on behalf of individuals when making decisions under the *Privacy Act*.[1] It looks at individuals who require, or choose to seek, assistance with their decision making. The need for the assistance may be because of a failing or fluctuating capacity to make decisions, to facilitate communication for non-English speakers or persons with a communicative disability, or merely for the convenience of the individual. The third parties involved may be carers, spouses, parents, adult children, interpreters, counsellors, legal representatives or any other person chosen by the individual. The arrangements may be temporary, one-off or short term arrangements, or permanent.

62.2 The establishment of such third party arrangements, with the consent of the individual, is consistent with the operation of the *Privacy Act*. There are concerns, however, that such arrangements are not consistently implemented or recognised by agencies and organisations. The ALRC proposes that the Office of the Privacy Commissioner (OPC) provide further guidance on appropriate practices and procedures that allow for the involvement of third parties to assist with making and communicating privacy decisions. This chapter also discusses whether there is a need to give arrangements involving decision making by third parties a legislative basis to ensure their recognition and provide additional protection for the individuals and third parties involved.

Problems with the *Privacy Act* in practice

62.3 A number of stakeholders noted examples of situations where third parties were denied access to the personal information of another individual, or otherwise stymied

1 Chapter 61 focuses on individuals who are incapable of making decisions.

in communicating with an agency or organisation, because of conflict, or perceived conflict, with the *Privacy Act*. These included:

- a person unable to assist a sick friend to make payments or defer payments on a phone service while the friend was in hospital;[2]
- widows and widowers having difficulties in changing financial details on joint accounts with banking institutions;[3]
- organisations refusing to accept a verbal authorisation of the individual to release personal information to lawyers, financial counsellors and interpreters;[4]
- a friend assisting an individual who speaks English as a second language, being denied access to personal information despite being in the same room as the consenting individual at the time a phone call was made;[5] and
- other third party assistants, including lawyers, financial counsellors and social workers, authorised to speak on behalf of the individual to negotiate suitable outcomes, but unable to access personal information about the individual.[6]

62.4 As discussed in Chapter 61, the Australian Guardianship and Administration Committee (AGAC) undertook a small survey in 2003–04 to determine whether there have been any unanticipated adverse consequences as a result of privacy legislation for people who have a decision-making disability.[7] Most of the concerns raised by AGAC related to the inflexible interpretation and application of privacy legislation by frontline staff involved in providing services. The New South Wales Disability Discrimination Centre suggested that narrow interpretation of privacy principles and a culture of 'risk minimisation' by frontline staff contribute to difficulties for people with a decision-making disability.[8]

62.5 Concerns and complaints about the impact of the *Privacy Act* on the ability of partners to assist each other with account facilitation and payments were also common comments received during the ALRC's National Privacy Phone-in held in June 2006.[9] One online contributor to the Phone-in stated:

> Current privacy laws are so heavily weighted against information flow that it is difficult for a modern family to operate effectively. What is classed as protection to some, is a hindrance to others. As a married man with children the levels of

2 K Bottomley, *Submission PR 10,* 1 May 2006.
3 B Such, *Submission PR 71,* 2 January 2007.
4 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.
5 Caroline Chisholm Centre for Health Ethics, *Submission PR 69,* 24 December 2006.
6 Legal Aid Queensland, *Submission PR 212,* 27 February 2007.
7 Australian Guardianship and Administration Committee, *Submission PR 129,* 17 January 2007.
8 NSW Disability Discrimination Legal Centre (Inc), *Submission PR 105,* 16 January 2007.
9 The National Privacy Phone-in is described in more detail in Ch 1.

> frustration my wife and I incur when trying to make enquiries or to alter contracts for phones, electricity, etc or anything really is way over the top. The amount of paper work that organisations claim to need under the umbrella of privacy is extreme. The number of times I am asked to put my wife on the phone or vice versa is an insult to us and hits at our own integrity … Privacy laws need to have some way of lifting all the restrictions married couples etc have to incur. It is not good enough to have a system where there are provisions for heaps of paperwork to be prepared. We are a family and should be treated as such.[10]

Existing third party arrangements

62.6 On its website, the OPC confirms that the *Privacy Act* does not prevent an agency or organisation from dealing with a third party authorised by an individual to act on his or her behalf.[11] The OPC goes on to note that different organisations have different procedures to ensure appropriate authorisation, including identity validation procedures. The OPC suggests that some organisations with existing customer verification procedures for telephone services may use such procedures for authorisation of third parties. The OPC also notes, however, that sometimes an organisation may decide that the circumstances and risk require a more robust authorisation process, such as the provision of written authorisation. Further guidance is not provided, although it is stated that the

> Privacy Commissioner would expect that if a customer was to follow the security and identification procedures an organisation uses in its ordinary dealings, and give their consent, a third party may be able to act on that customer's behalf.[12]

62.7 A number of agencies and organisations have adopted third party arrangements as part of their normal course of business. For example, Optus has a procedure for establishing a third party authority nominated by the account holder to act on his or her behalf. A nominated person can request, change and supply information regarding the account. A nominated person cannot, however, do any action that requires the account holder's signature or verbal electronic authorisation, including changing personal details or activating a new service.[13] Optus notes that, in some cases, third party access is the primary form of communication between Optus and the customer, especially for customers with a disability or those from a non-English speaking background.[14] Telstra

---

10 *ALRC National Privacy Phone-in*, June 2006, Comment #778.

11 Office of the Privacy Commissioner, *FAQs: Can I Authorise Someone to Act on My Behalf when Dealing with a Business?* <www.privacy.gov.au/faqs/ypr/q14.html> at 17 July 2007.

12 Ibid.

13 A full list of actions that cannot be undertaken by a nominated person are set out at Optus, *Personal—Mobile Account Access* <www.optus.com.au> at 17 July 2007 and Optus, *Small Business—Third Party Access* <www.optus.com.au> at 17 July 2007. Where a power of attorney is granted for general purposes, and the legal document establishing the power of attorney is sighted by an Optus customer service representative, the nominated person will have the same level of access to an account as the account holder.

14 Optus, *Personal—Mobile Account Access* <www.optus.com.au> at 17 July 2007; Optus, *Small Business—Third Party Access* <www.optus.com.au> at 17 July 2007.

also has a system for naming an 'authorised representative' who is able to access information about an account on behalf of the legal lessee.[15] MBF Health has an option for nominating a person to undertake membership transactions, collect benefits, or both, on behalf of the primary member. The nominee has the same rights and obligations as the primary member, including access to the health information of all persons on the membership.[16]

62.8 As noted in Chapter 61, Centrelink has nominee arrangements that are underpinned by legislation.[17] Individuals can nominate any third party to act on their behalf in one or more of the following ways: to make enquiries only; to receive payments (payment nominee); or to act and make changes generally (correspondence nominee). Forms and processes for nominee arrangements are also used by Centrelink to recognise formal decision-making relationships for individuals without capacity.

62.9 The Centrelink nominee arrangements have operated administratively in the past, although were given a legislative basis in 2002. On introduction of the provisions, the need for a legislative basis was explained as follows:

> The amendments relating to nominees form a part of the measures being undertaken to give effect to the Government's commitment to implement a simpler and more coherent social security system.
>
> Nominees are particularly relevant to youth allowance, age pension and disability support pension recipients who have difficulty managing their own financial affairs.
>
> Currently, the law only provides for a payment nominee and arrangements relating to correspondence are dealt with administratively. Similarly, the current law does not clearly set out the duties and obligations of nominees. With an ageing population the use of nominees is likely to increase so it is considered appropriate to address these issues now.[18]

62.10 Part 3A of the *Social Security (Administration) Act 1999* (Cth) provides the detail for the operation of the nominee arrangements, including the functions and responsibilities of nominees. In particular, the payment or correspondence nominee has a duty to act at all times in the best interests of the principal beneficiary.[19] There is also provision for the suspension or revocation of nominee appointments.[20]

---

15 Telstra, *Access for Everyone: Your A–Z Guide* (2006).

16 MBF Health, *Form: Partner Authority/Application for Legal Authority*.

17 *Social Security (Administration) Act 1999* (Cth) pt 3A, which was inserted by the *Family and Community Services Legislation Amendment (Budget Initiatives and Other Measures) Act 2002* (Cth).

18 Explanatory Memorandum, Family and Community Services Legislation Amendment (Budget Initiatives and Other Measures) Bill 2002 (Cth), i. It was suggested to this Inquiry, however, that a legislative basis is not necessary for the operation of nominee arrangements consistent with the *Privacy Act*: Australian Government Department of Families Community Services and Indigenous Affairs, *Submission PR 162,* 31 January 2007.

19 *Social Security (Administration) Act 1999* (Cth) s 123O.

20 Ibid s 123E.

62.11 These examples of nominee arrangements generally facilitate an ongoing relationship between the individual and the nominated third party. They do not cover one-off or short term relationships. Such relationships could include a professional service provider, such as a counsellor, legal representative, or interpreter, where the professional is involved to assist the individual to make a decision, rather than make the decision on behalf of the individual. It may be necessary, however, for the service provider to have access to appropriate personal information about the individual in order to provide the required assistance. Other circumstances may involve one-off or short term arrangements made by an individual during a particular period—perhaps because of an illness or overseas trip.

62.12 In all of these circumstances, the *Privacy Act* provides for disclosure of personal information about an individual where the individual has provided consent. There is no reason why an agency or organisation could not provide a mechanism for acknowledging the consent of the individual and disclosing the necessary personal information to the nominated third party in accordance with that consent. This would cover circumstances where the third party is assisting the individual, but the individual makes decisions based on the information.

62.13 There may be complications, however, where there is a need to recognise a third party able to make decisions on behalf of the individual. There is no existing mechanism in the Act which provides for a third party, even with the consent of the individual, to make a decision under the Act on behalf of the individual. As noted above, the OPC has stated that it sees no barrier to organisations dealing with third parties authorised by the individual.[21]

62.14 In Chapter 61, the ALRC proposes the establishment of an 'authorised representative' mechanism that allows an appropriate third party to make decisions on behalf of an individual who is not capable of making the decision.[22] The ALRC is examining whether the definition of an authorised representative should include a person nominated by the individual to make decisions on his or her behalf before becoming incapable of making a decision.[23] The ALRC's proposed authorised representative mechanism is, however, only intended to operate where, despite assistance being given, the individual is found not to be capable of making the decision. This is to ensure that individuals are given the maximum opportunity to be involved in decisions about themselves and, wherever possible, make their own decisions. The mechanism has appropriate safeguards built in to protect the most vulnerable individuals. It is not intended to cover the circumstance of a nominated third

---

21 Office of the Privacy Commissioner, *FAQs: Can I Authorise Someone to Act on My Behalf when Dealing with a Business?* <www.privacy.gov.au/faqs/ypr/q14.html> at 17 July 2007.

22 Proposals 61–1, 61–2.

23 Question 61–2.

party making decisions on behalf of an individual who is capable of making decisions under the Act.

62.15 Even if the *Privacy Act* recognised the ability of a nominated third party to make decisions under the Act with the consent of the individual, this would not necessarily allow the third party to make all decisions concerning a particular service or transaction with an agency or organisation. Agencies and organisations may be subject to other obligations, such as the bankers' duty of confidentiality or particular legislative provisions, which do not allow for third party decision making. Each agency and organisation must give consideration to the extent to which it is able to recognise and act upon decisions made by a nominated third party. Some circumstances require a more rigorous process for nomination and verification than others due to the potential consequences of the disclosure of personal information or the transaction involved.

ALRC's view

62.16 The ALRC considers that appropriate implementation of third party arrangements is a practical way to provide flexibility for individuals—to ensure that individuals continue to receive the protections offered by the *Privacy Act* while not unduly inhibiting communication with, and access to benefits and services from, agencies and organisations. The *Privacy Act* does not prevent the operation of such arrangements. There is, however, evidence to suggest that third party arrangements are not being implemented properly. This is contributing to the perception that the *Privacy Act* is often a barrier to accessing benefits and services.

62.17 A common theme in submissions and consultations is that frontline staff do not understand fully the operation of the *Privacy Act*, and often adopt risk averse behaviour to ensure their obligations under the Act are met. Unfortunately, while well intended, such behaviour can lead to frustration for individuals and their nominated third parties, and infringe the rights of the individual by hindering access to personal information about him or her.

62.18 A number of the ALRC's proposals are intended to clarify the provisions of *Privacy Act* and improve understanding for agencies, organisations and individuals about how the Act should operate in practice.[24] This is an area, however, where the ALRC sees the need for particular guidance to be developed and published by the OPC. The guidance should provide direction on appropriate practices and processes recognising and providing for third party arrangements that should be adopted by agencies and organisations. It should cover short term and long term arrangements, and situations where the third party is merely assisting the individual as well as where the nominated third party can make decisions on behalf of the individual. An assortment of

24 These proposals include harmonisation of information privacy laws across jurisdictions (Proposals 4–1, 4–2, 4–3, 4–4, 4–5), amendment of the Act to achieve greater logical consistency, simplicity and clarity (Proposal 3–2), inclusion of an objects clause in the Act (Proposal 3–4), and a variety of proposals for the OPC to undertake particular education campaigns (see summary in Ch 44).

processes could be adopted, including over the phone consent and identification verification, online verification and written nomination processes. The guidance should assist agencies and organisations to recognise the kinds of processes that might be suitable for a particular situation. Such guidance would provide agencies and organisations with the confidence to introduce appropriate arrangements that are consistent with the *Privacy Act*, and ensure that staff are trained appropriately to implement the arrangements.

62.19 There is a solid basis in the Act for allowing disclosure of personal information to third parties with the consent of the individual. The ALRC questions, however, whether the *Privacy Act* gives sufficient recognition to nominated third parties making decisions on behalf of a capable individual. The *Privacy Act* does not prevent the recognition of nominated third parties. Express recognition in the Act of nominated third parties, however, would provide further impetus and confidence for agencies and organisations to implement appropriate third party arrangements that involve decision making.

62.20 The ALRC is interested in receiving further input on whether it is desirable to enact a legislative provision that provides for nominated third parties making decisions on behalf of capable individuals, and whether the provision should set out the obligations of a nominated third party.

Proposal 62–1 Practice and procedures allowing for the involvement of third parties to assist an individual to make and communicate privacy decisions should be developed and published in guidance issued by the Office of the Privacy Commissioner.

Question 62–1 Should the *Privacy Act* be amended expressly to allow a third party nominated by the individual to give consent, make a request or exercise a right of access on behalf of the individual, either for one-off or long term arrangements?

Part J

Telecommunications

63. *Telecommunications Act*

Contents

Introduction 1849
Telecommunications Act 1997 (Cth) 1851
Are two privacy regimes necessary? 1853
Does the *Telecommunications Act* provide adequate privacy protection? 1858
Interaction between the *Privacy Act* and the *Telecommunications Act* 1859
Exceptions to the use and disclosure offences 1860
- Performance of person's duties 1860
- Required or authorised by or under law 1861
- Law enforcement and the protection of public revenue 1863
- Threat to person's life or health 1868
- Knowledge of person concerned 1869
- Consent 1871
- Implicit consent 1872
- Business needs of other carriers or service providers 1873
- Credit reporting information and credit worthiness 1876

Integrated public number database 1878
- Public number directories not sourced from the IPND 1884
- Are public number directories desirable? 1886

Small business exemption 1889
Criminal or civil penalties 1891
New technologies 1892
Telecommunications regulators 1895
- Guidance 1896
- Codes and standards 1896
- Reporting 1898

A redraft of the Part 1899

Introduction

63.1 Telecommunications providers collect personal information about their customers in order to supply them with services such as landline telephone services, mobile telephone services and internet services. Before the introduction of the private sector provisions of the *Privacy Act 1988* (Cth), the use and disclosure of information collected and held by telecommunications providers was regulated by industry-specific

legislation[1] and instruments.[2] Since the introduction of the private sector provisions, however, the handling of personal information by telecommunications providers is governed by both the *Telecommunications Act 1997* (Cth) and the *Privacy Act*, as well as other industry-specific instruments, such as licences and codes.

63.2 A number of recent inquiries have considered the interaction between the telecommunications industry-specific regulation and the *Privacy Act.* In 2005, the Office of the Privacy Commissioner (OPC) considered this interaction as part of its review of the private sector provisions of the *Privacy Act* (OPC Review).[3] The OPC's recommendations on this issue are discussed throughout this chapter.

63.3 In 2005, the Senate Legal and Constitutional References Committee concluded an inquiry into the *Privacy Act* (Senate Committee privacy inquiry). One of its recommendations was that the ALRC conduct a comprehensive review of privacy that considered, among other things, the interaction between the *Privacy Act* and the *Telecommunications Act*.[4] In addition, in 2006 a review of the regulation of business in Australia concluded that the need to clarify and harmonise the relationship between the *Privacy Act* and the *Telecommunications Act* should be considered as part of a wider review of privacy laws.[5]

63.4 On 8 May 2006, the ALRC received a letter from the Attorney-General, the Hon Philip Ruddock MP, stating that it would be desirable for the ALRC to consider the interaction between the *Privacy Act* and the *Telecommunications Act* during the course of this Inquiry.

63.5 This chapter first considers whether telecommunications-specific privacy legislation is still required. The next section examines how the *Telecommunications Act* interacts with the *Privacy Act*. The chapter then looks at whether the *Telecommunications Act* provides adequate protection of personal information. The final section of the chapter considers the role of the OPC and the Australian Communications and Media Authority (ACMA) under the *Telecommunications Act*.

63.6 Chapter 64 considers the *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth), *Telecommunications (Interception and Access) Act 1979* (Cth) and the functions of the various bodies with responsibility for privacy in the telecommunications industry. The privacy of internet users and users of wireless technologies is discussed more generally in Chapter 6.

---

1 *Telecommunications Act 1991* (Cth) s 88; *Telecommunications Act 1997* (Cth) pt 13.

2 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) (de-registered on 29 Oct 2001); *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

3 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005).

4 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), recs 1, 9.

5 Regulation Taskforce 2006, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer (2006), rec 4.48.

Telecommunications Act 1997 (Cth)

63.7 The *Telecommunications Act* regulates the activities of a number of participants in the telecommunications industry, including 'carriers' and 'carriage service providers'. The statutory definitions of these terms are complex. Essentially, a 'carrier' is the holder of a 'carrier licence'[6]—a type of licence required before certain infrastructure can be used to carry communications by means of guided and/or unguided electromagnetic energy.[7] A 'carriage service provider' is a person who makes use of the infrastructure owned by a carrier to carry these types of communications.[8]

63.8 Part 13 of the *Telecommunications Act* regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunication services. It makes it an offence (punishable by up to two years imprisonment) for certain participants in the telecommunications industry—namely, carriers, carriage service providers, telecommunications contractors and employees of carriers, carriage service providers and telecommunications contractors; eligible number-database operators;[9] and emergency call persons—to use or disclose information relating to the:

- contents of a communication carried, or being carried, by a carrier or carriage service provider;
- carriage services supplied or intended to be supplied by a carrier or carriage service provider; or
- affairs or personal particulars (including any unlisted telephone number or any address) of another person.[10]

63.9 The Act specifies a number of exceptions to these 'primary use/disclosure offences'.[11] The Act also regulates the secondary use and disclosure of protected information.[12] For example, a person to whom information was disclosed because the disclosure was required or authorised by law is prohibited from using or disclosing the information, unless the further use and disclosure is also required or authorised by law.[13] A person who contravenes the secondary use and disclosure provisions is also guilty of an offence punishable by up to two years imprisonment.[14]

63.10 Part 6 of the *Telecommunications Act* deals with the development of industry codes and standards for particular industry activities. Industry codes and standards

---

6 *Telecommunications Act 1997* (Cth) s 7. A carrier licence is granted under s 56 of the Act.
7 Ibid ss 7, 42.
8 Ibid ss 7, 16, 87.
9 Ibid s 272. There are currently no eligible number database operators as no determination is in force under s 472(1).
10 Ibid ss 276–278.
11 Ibid ss 279–294. These exceptions are discussed in detail below.
12 Ibid ss 296–303A.
13 Ibid s 297.
14 Ibid s 303.

developed under the Act can deal with privacy, including the protection of personal information.[15] An industry code or standard cannot, however, derogate from the requirement of the *Privacy Act* or a privacy code approved under the *Privacy Act*.[16]

63.11 The *Telecommunications Act* requires telecommunications providers to record and report to ACMA on certain disclosures of information under the Act.[17] In 2005–06, participants in the telecommunications industry made 944,367 reported disclosures pursuant to exceptions under Part 13 of the *Telecommunications Act*. This was an increase of 58,901 or 6.23% cent over the previous reporting year.[18] ACMA reported that, while the overall trend has been towards increasing disclosures, in 2005–06 disclosures in most categories decreased marginally.[19]

63.12 Among the major carriers, Telstra makes more reported disclosures than the other carriers, both because of its market share and because of its role as the Integrated Public Number Database Manager. In 2005–06, Telstra made 74% of the disclosures reported under Part 13 of the *Telecommunications Act*. Among the other carriers, Virgin Mobile made 7%, Vodafone made 6%, Optus made 5% and other carriage service providers made 8%.[20]

63.13 The *Privacy Act* regulates many aspects of the handling of personal information by telecommunications providers. For example, a telecommunications provider that is not a small business will have to collect information in compliance with National Privacy Principle 1 (NPP 1), and will have to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date as required under NPP 3. Thus, both Part 13 of the *Telecommunications Act* and the NPPs regulate the use and disclosure of personal information. The interaction between these provisions is discussed further below.

63.14 In 1999, the Australian Communications Industry Forum (ACIF) (now Communications Alliance), a body that represents the interests of the communications industry, developed and registered the *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* (the Code) under Part 6 of the *Telecommunications Act*.[21] The Code expanded on the privacy protections of Part 13 and addressed matters that are not dealt with in the Part, such as how information should be collected, stored and handled. These requirements were based on the National Principles for the Fair Handling of Personal Information, which later became

---

15 Ibid s 113(3)(f).
16 Ibid s 116A.
17 Ibid ss 306, 308. The Act does not require uses to be reported.
18 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145. In 2004–05, there were 885,466 reported disclosures—an increase of 26% from the previous financial year: Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 186. The *Telecommunications Act* does not require all disclosures to be reported.
19 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145.
20 Ibid, 146.
21 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999).

the NPPs under the *Privacy Act*. The Code was considered to be unnecessary when the private sector provisions of the *Privacy Act* came into force and was deregistered in 2001.

Are two privacy regimes necessary?

63.15 A threshold question is whether two privacy regimes are necessary in the telecommunications industry, or whether the industry should be regulated under telecommunications-specific privacy laws or the *Privacy Act*.

Submissions and consultations

63.16 It was argued in a number of submissions that telecommunications-specific privacy laws are necessary. Some stakeholders noted that Part 13 of the *Telecommunications Act* and the *Privacy Act* have different purposes. While the *Privacy Act* sets out various rights of individuals in relation to the handling of their personal information, Part 13 is directed more towards deterrence and punishment.[22]

63.17 Stakeholders also noted that Part 13 deals with many aspects of the telecommunications industry that are not addressed by the *Privacy Act*. For example, the Australian Government Department of Communications, Information Technology, and the Arts (DCITA) submitted that the content and substance of communications and unlisted numbers require industry-specific privacy regulation because they will not always be protected under the *Privacy Act*.[23] It was also noted that the telecommunications industry has access to vastly more information about individuals than most organisations, including information about their own customers and other members of the general public. Such information includes the content of their communications.[24]

63.18 The Office of the Victorian Privacy Commissioner (OVPC) submitted that telecommunications regulation is an area where fragmentation is a positive thing.

> Care should be taken not to ask or expect all things from generic privacy laws or from a single regulator. Here, separate regulation with purpose-built protections is desirable as it covers intrusive activities (eg listening in to telephone conversations) that may not generate any records. Privacy legislation is essentially about protecting documents or records, not transmissions.[25]

63.19 It was submitted that the *Telecommunications Act* permits the use and disclosure of personal information where it is necessary for the efficient functioning of the

---

22 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. See also Australian Federal Police, *Submission PR 186,* 9 February 2007.

23 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

24 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

25 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007. See also Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

telecommunications industry. For example, the telecommunications sector relies on the interconnection of different telecommunication networks in order to enable a consumer to communicate with any other user, regardless of the networks to which those end-users are connected. Accordingly, exceptions under Part 13 of the *Telecommunications Act* that go beyond those available under the *Privacy Act* are necessary to enable industry networking arrangements to work efficiently and effectively.[26]

63.20 It was noted in other submissions, however, that much of the information used and disclosed in the telecommunications industry could be regulated under the *Privacy Act*. It was submitted that in most cases the personal information collected by telecommunications providers is no different to personal information collected in other sectors. This information will often be obtained in the course of business but will not be related directly to the carriage of telecommunications services.[27] For example, personal information held by a telecommunications company, a bank or an electricity provider in relation to any given customer is likely to be broadly similar—it would include identifying information such as the individual's name, address, telephone number and other contact information; as well as other information such as billing history, credit card details and likely income level.[28]

63.21 A number of submissions also noted that due to technological and market 'convergence',[29] the boundaries between the telecommunications industry and other related industries are starting to blur.

> Increasingly, communications and related services will rely on a range of intermediate services and databases. If differences in the treatment of personal information persist between 'telecommunications' services and other businesses, the potential for unintended outcomes and for difficulties in administration across regulatory boundaries will increase markedly. This will become increasingly problematic as communications becomes embedded in more and more services.[30]

63.22 The communications industry is also experiencing business diversification, specialisation and the entry of new niche industry participants. The lower cost of creating and distributing digitalised content and communications is lowering barriers to market entry and resulting in the emergence of new online services and environments.[31]

---

26 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

27 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

28 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

29 'Convergence' refers to a range of different technologies performing similar tasks. An example of a 'convergent device' is the mobile phone and other mobile communications devices that can act as multimedia platforms and, in particular, deliver audiovisual content. See Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 21; Australian Government Department of Communications Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006).

30 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007. See also Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

31 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 22.

63.23 Stakeholders outlined a number of options for reform. It was suggested in one submission that the development of an instrument focused on telecommunications privacy would be appropriate.[32] The European Union has taken steps to regulate specifically the handling of data by the telecommunications industry. For example, the 2002 Directive on privacy and electronic communications requires Member States to, among other things, enact legislation to ensure the confidentiality of telecommunications and telecommunications data,[33] and to ensure that subscribers to telecommunication services are given the opportunity to determine whether their personal data are included in a public directory.[34] The 2006 data retention Directive aims to ensure that telecommunications data are retained for a certain period in case they are required for law enforcement purposes.[35] It also requires Member States to ensure that data are stored securely, and destroyed at the end of the retention period.[36]

63.24 Another stakeholder argued that the deregistration of the ACIF *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* has resulted in regulatory gaps in the protection of personal information in the telecommunications industry. It was also noted that deregistration of the Code has resulted in a number of small telecommunications businesses not being regulated by any privacy rules as they are not covered by the *Privacy Act*.[37] AAPT suggested that one option would be the development of an overarching document, whether a code, guide or separate piece of legislation, that provides a comprehensive overview of telecommunications privacy.[38] Others submitted, however, that the development of a telecommunications specific industry privacy code is likely to result in additional compliance cost and a greater overlap with existing regulation.[39]

63.25 The OPC submitted that consideration should be given to removing the exceptions under Part 13 (while keeping the Part 13 offence provisions), and allowing the *Privacy Act* to regulate use and disclosure under that Part. Others suggested that Part 13 could be moved into the *Privacy Act*, perhaps as an industry-specific section of the Act.[40] Stakeholders also suggested that privacy regulation applying to the telecommunications sector should be aligned with the general privacy provisions contained in the *Privacy Act*, particularly in the area of exemptions and penalties.[41] The

---

32 K Pospisek, *Submission PR 104,* 15 January 2007.

33 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002), art 5.

34 Ibid, art 12.

35 European Parliament, *Directive on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks*, Directive 2006/24/EC (2006), art 1.

36 Ibid, art 7.

37 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

38 AAPT Ltd, *Submission PR 87,* 15 January 2007.

39 Telstra, *Submission PR 185,* 9 February 2007.

40 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

41 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

OPC Review noted the possibility of amending the *Telecommunications Act* and the *Privacy Act* to ensure the highest of the two standards always operates.[42]

ALRC's view

63.26 The ALRC considers that both the *Telecommunications Act* and the *Privacy Act* should regulate privacy in the telecommunications industry. The telecommunications industry handles sensitive personal information. In addition to information such as financial information, telephone numbers and other contact information, telecommunications providers hold information about when, how and with whom individuals communicate, and the content of those communications. In the ALRC's view, it is appropriate that the use and disclosure of this information is subject to more stringent laws than the *Privacy Act*.

63.27 The *Telecommunications Act* protects a broader category of information than the *Privacy Act*. The *Privacy Act* regulates only personal information held in a 'record'.[43] In contrast, Part 13 of the *Telecommunications Act* regulates information that may or may not be held in a 'record', including information that relates to the contents or substance of a communication.[44] Further, Part 13 of the *Telecommunications Act* does not regulate all stages of the information-handling cycle. These matters are dealt with under the *Privacy Act*. The ALRC considered whether it would be appropriate for the regulation of 'personal information' to be removed from *Telecommunications Act*. The ALRC believes, however, that this would only create confusion and further fragment the regulation of the telecommunications industry.

63.28 The ALRC also notes that specific exemptions to the offence provisions which go beyond those available under the *Privacy Act* are necessary to enable industry networking arrangements to work efficiently and effectively. The ALRC considered whether telecommunication-specific exceptions under the *Privacy Act* could accommodate these uses and disclosures. It is the ALRC's view, however, that this would add another layer of complexity to privacy regulation in the telecommunications industry.

63.29 In the ALRC's view, the interaction between the *Telecommunications Act* and the *Privacy Act* should be clarified. The ALRC's approach to reform in this area involves:

- clarification of the interaction between the *Telecommunications Act* and the *Privacy Act*;

---

42 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007. Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 60.

43 See the *Privacy Act 1988* (Cth) s 16B. 'Record' is defined under s 6 of the *Privacy Act 1988* (Cth).

44 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

- clarification of the scope of the exceptions to the use and disclosure offences under the *Telecommunications Act*;

- the alignment of the exceptions to the use and disclosure offences under the *Telecommunications Act* with the exceptions under the proposed 'Use and Disclosure' principle in the *Privacy Act*;

- ensuring that all participants in the telecommunications industry are subject to privacy regulation;

- the development of guidance relating to privacy in the telecommunications industry that addresses the interaction between the *Telecommunications Act* and the *Privacy Act*; and

- greater cooperation between the bodies with responsibility for privacy regulation in the telecommunications industry.

63.30 The ALRC acknowledges the need for telecommunications regulation to respond to a convergent communications environment. This has been a theme in a number of recent reports and inquiries.[45] In Australia there are currently a number of regulatory frameworks that apply to information according to the communications platform over which it is delivered.[46]

63.31 In the ALRC's view, issues related to convergence extend beyond the terms of reference for this Inquiry. The ALRC, therefore, proposes that the Australian Government should initiate a review to consider the extent to which the *Telecommunications Act* continues to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and shifting community perceptions and expectations about communication technologies.[47] This review should consider other legislation that regulates the telecommunications industry and how it interacts with the *Telecommunications Act*, including the *Telecommunications (Interception and Access) Act.*[48]

63.32 The proposed review should also consider the extent to which the activities regulated under the *Telecommunications Act* and the *Telecommunications (Interception and Access) Act* should be regulated under general communications legislation or other

---

45 See, eg, Australian Government Department of Communications Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006); Australian Communications Authority, *Vision 20/20: Future Scenarios for the Communications Industry—Implications for Regulation* (2005).

46 See, eg, *Telecommunications Act 1997* (Cth); *Broadcasting Services Act 1992* (Cth).

47 See Senate Environment Communications Information Technology and the Arts References Committee, *A Lost Opportunity? Inquiry into the Provisions of the Australian Communications and Media Authority Bill 2004 and Related Bills and Matters* (2005), rec 1.

48 The *Telecommunications (Interception and Access) Act 1979* (Cth) is discussed in Ch 64.

legislation; and the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including ACMA, the Attorney-General's Department, the OPC, the Telecommunications Industry Ombudsman (TIO), and Communications Alliance. The ALRC notes that the amalgamation of key broadcasting and telecommunications regulators in the United Kingdom provided the opportunity to establish a new regulatory framework under the *Communications Act 2003* (UK).

Proposal 63–1 The Australian Government should initiate a review to consider the extent to which the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how the Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation; and

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Australian Government Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance.

Does the *Telecommunications Act* provide adequate privacy protection?

63.33 In IP 31, the ALRC asked whether the *Telecommunications Act* provides adequate and effective protection for the use, disclosure and storage of personal information.[49] The ALRC also asked whether any issues are raised by the interaction between the *Privacy Act* and the *Telecommunications Act*.[50]

49 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 10–1.
50 Ibid, Question 10–2.

63.34 One stakeholder submitted that the *Telecommunications Act* operates effectively in tandem with the *Privacy Act*.[51] Other stakeholders, however, raised a range of issues related to telecommunications privacy regulation including: confusion about how the two Acts interact; lack of clarity around the exceptions to the use and disclosure offences; inadequate protection of personal information held on public number directories; regulatory gaps caused by the small business exemption; the impact of new privacy-invasive technologies; and the role and function of the various bodies with responsibility for telecommunications privacy.

Interaction between the *Privacy Act* and the *Telecommunications Act*

63.35 The *Privacy Act*, and in particular the NPPs, continue to regulate many aspects of the handling of personal information by telecommunications providers. For example, a telecommunications provider can only collect personal information that is necessary for one or more of its functions or activities, such as to enable the provision of telecommunication services to a customer and to facilitate the billing for those services.[52] In addition, a telecommunications provider must take reasonable steps to ensure that an individual is aware of certain matters at or around the time of collection, such as the types of organisations to which the provider usually discloses the information.[53]

63.36 NPP 2 and Part 13 of the *Telecommunications Act* regulate the use and disclosure of personal information. As noted above, Part 13 makes it an offence to use or disclose certain information, subject to a number of exceptions. These exceptions provide the *only* circumstances in which it is lawful for those regulated by the *Telecommunications Act* to use or disclose that information. Therefore, the exceptions under NPP 2 that permit uses and disclosures that are not permitted under Part 13 will not apply.

63.37 On the other hand, an organisation that uses or discloses personal information in a way that is authorised under the *Telecommunications Act* will not be in breach of NPP 2. An act or practice engaged in pursuant to any of the exceptions under Part 13 is an act or practice that is 'authorised by or under law' for the purposes of NPP 2 and the proposed 'Use and Disclosure' principle.[54] This is confirmed by s 303B of the *Telecommunications Act,* which provides that a use or disclosure permitted under that Act is a use or disclosure that is 'authorised by law' for the purposes of the *Privacy Act.*[55]

---

51 Telstra, *Submission PR 185,* 9 February 2007.
52 *Privacy Act 1988* (Cth), sch 3, NPP 1.1.
53 See Ibid sch 3, NPPs 1.3, 1.5.
54 See Ch 22.
55 *Telecommunications Act 1997* (Cth) s 303B.

63.38 Conversely, if a participant in the telecommunications industry engages in an act or practice that does not comply with one of the exceptions under Part 13, the act or practice would not be 'authorised by or under law' and so may breach NPP 2 and the proposed 'Use and Disclosure' principle.[56] This is supported by s 303C of the *Telecommunications Act*, which provides that a prosecution for an offence relating to the use or disclosure of protected information under the *Telecommunications Act* does not prevent civil proceedings or administrative action being taken under the *Privacy Act* for the same breach.[57]

Exceptions to the use and disclosure offences

63.39 The exceptions under Part 13 of the *Telecommunications Act* provide for a range of circumstances in which carriers and carriage service providers may use or disclose personal information. It has been argued that many of the exceptions are unnecessarily broad and do not provide a sufficient level of protection of personal information in the telecommunications industry.[58] This section of the chapter considers a number of issues raised in submissions relating to these exceptions and whether they can be aligned more closely with the exceptions to the proposed 'Use and Disclosure' principle.

Performance of person's duties

63.40 Sections 279 and 296 of the *Telecommunications Act* provide that the primary and secondary use and disclosure of information is permitted if the use or disclosure is made in the performance of that person's duties as an employee[59] or contractor.[60] It has been noted that the exception is necessary for 'the myriad of day-to-day communications between employees about connecting, disconnecting and billing customers'.[61]

63.41 AAPT submitted that the exception seems to imply that as long as someone is an employee of a supplier, and is embarking on duties associated with that employment, then they can use and disclose personal information in any way they see fit.

---

56 An act or practice that is prohibited under the *Telecommunications Act* may also be permitted under one of the other exceptions to NPP 2. This does not permit the act or practice as Part 13 still applies to the use or disclosure of that information.

57 *Telecommunications Act 1997* (Cth) s 303C.

58 Electronic Frontiers Australia Inc, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, [30]–[51]. See also AAPT Ltd, *Submission PR 87,* 15 January 2007.

59 An employee of a carrier, carriage service provider, telecommunications contractor, number-database operator, number-database contractor, a person who operates an emergency call service or an emergency call contractor: *Telecommunications Act 1997* (Cth) s 279(1), (3), (5).

60 A telecommunications contractor, number-database contractor or an emergency call contractor: Ibid s 279(2), (4), (6).

61 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 6. An eligible person or an eligible number-database person is not required to report to ACMA the number of disclosures they make under ss 279 and 296: *Telecommunications Act 1997* (Cth) s 306(1).

> We are confident that this is not the intended reading of this section, and it is entirely at odds with the *Privacy Act 1988* and its requirements when it comes to the use and disclosure of personal information.
>
> The Act also leaves itself open to interpretation about what we consider are key privacy consumer protection mechanisms. This includes not allowing Sales and Marketing people to use the detail of a call to attempt to market to these customers based on these details.[62]

63.42 The ALRC acknowledges that an exception to this effect is necessary to enable industry networking arrangements to work efficiently and effectively. In the ALRC's view, however, the scope of the present exception is unclear. One option would be to amend ss 279 and 296 to confine the exception to certain duties of an employee or contractor, including connecting and disconnecting telecommunication services or billing.

63.43 Another option would be a requirement that a use or disclosure by a person made for the purpose of performing that person's duties must be related to the primary purpose of collection. This would bring the exception more closely into line with the proposed 'Use and Disclosure' principle, under which an agency or organisation may use or disclose personal information for a purpose (the secondary purpose) other than the primary purpose of collection if both of the following apply, the:

- secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
- individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.[63]

63.44 The ALRC is interested in stakeholder views on this issue.

Question 63–1 Sections 279 and 296 of the *Telecommunications Act 1997* (Cth) permit the use or disclosure by a person of information or a document if the use or disclosure is made 'in the performance of the person's duties' as an employee or contractor. Is the exception too broadly drafted? Is it resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined?

Required or authorised by or under law

63.45 Sections 280(1)(b) and 297 provide that a primary or secondary use or disclosure of information or document is permitted if the use or disclosure is required

62 AAPT Ltd, *Submission PR 87,* 15 January 2007.
63 See Ch 22.

or authorised by or under law. NPP 2 and the proposed 'Use and Disclosure' principle provide for a similar exception.[64] ACMA has reported that 13,634 disclosures were made under s 280 in 2005–06.[65]

63.46 Submissions highlighted that one possible interpretation of s 280(1)(b) is that a telecommunications company could rely on the exceptions under NPP 2 to disclose information (for example, for direct marketing) in addition to those under Part 13 of the *Telecommunications Act*.[66] The OPC submitted that both the *Privacy Act* and the *Telecommunications Act* should be amended to ensure that the *Privacy Act* cannot be used to lower the standard of privacy protection provided by the *Telecommunications Act*.[67]

63.47 In the ALRC's view, ss 280(1)(b) and 297 should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the proposed 'Use and Disclosure' principle under the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

63.48 In Chapter 13, the ALRC considers the scope of the 'required or authorised by or under law' exception in the context of the *Privacy Act*. In that chapter the ALRC notes that the scope of the exception requires clarification. The ALRC notes that legislation should set out clearly whether it is intended to require or authorise an act or practice for the purposes of the exception. The ALRC also discusses the compilation of a list of provisions in other legislation that require or authorise acts or practices for the purposes of the exception. The ALRC is interested in hearing stakeholder views on whether this option would help to clarify the scope of the exception under ss 280(1)(b) and 297.

Proposal 63–2 Sections 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the proposed 'Use and Disclosure' principle under the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

---

64 Rule 6.1(c)(f) of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) provided an identical exception. The scope of the 'required or authorised by or under law' exception in the context of the *Privacy Act 1988* (Cth) is discussed in Chapter 13.

65 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145.

66 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

67 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 2.4.8.

Law enforcement and the protection of public revenue

63.49 Section 282 of the *Telecommunications Act* provides that the use or disclosure by a person of information is not prohibited if the use or disclosure is reasonably necessary for certain law enforcement purposes, including the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty or the protection of public revenue.[68] This exception requires the relevant person, for example an employee of the telecommunications provider, to make a judgement as to whether the disclosure or use is necessary for that purpose. The Explanatory Memorandum to the Telecommunications Bill 1996 (Cth) noted that this exception is necessary

> to allow disclosure where a carrier employee comes across information which clearly is relevant to enforcement of the criminal law in the course of performing his or her duties and the information has not been requested by a law enforcement agency.[69]

63.50 The Explanatory Memorandum notes, however, that the exception had created difficulties for employees who are not in a position to be able to make an objective judgment about whether disclosure is reasonably necessary because they do not know the details of the investigation. The *Telecommunications Act* therefore introduced a new test which enables an eligible person to disclose information where an authorised officer has certified that the disclosure is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue.[70] In these cases, it is the relevant authorised certifying officer, not the telecommunications provider, who makes the judgement as to whether the disclosure is necessary.[71] Section 283 of the *Telecommunications Act* provides a similar exception in relation to disclosures made to the Australian Security and Intelligence Organisation (ASIO). ACMA has reported that 944,367 disclosures were made under the 'enforcement of law' exception under s 282 of the *Telecommunications Act* in 2005–06.[72]

63.51 Under s 282(6) a certificate cannot authorise the disclosure of information or a document relating to the contents or substance of a communication that has been carried, or is in the process of being carried, by a carrier or carriage service provider. This indicates a legislative intention that such information can only be obtained by a warrant under the *Telecommunications (Interception and Access) Act*.

63.52 In 2005, a report on a review of regulation of access to communications conducted by Mr Anthony Blunn (the Blunn Report) observed of s 281(1) and (2):

---

68 *Telecommunications Act 1997* (Cth) s 282(1), (2)

69 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 7.

70 *Telecommunications Act 1997* (Cth) s 282 (3), (4), (5).

71 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 7.

72 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145. In 2004–05, there were 885,466 disclosures—an increase of 26% from the previous financial year: Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 186.

> In as much as they require the eligible person to form an opinion that disclosure is 'reasonably necessary' for the enforcement of the criminal law or the protection of the public revenue they appear inappropriate and sit oddly with the requirement established by subsections 282(3), (4) and (5) for a certificate from the requesting agency in which case access to content or substance is precluded.[73]

63.53 The Blunn Report acknowledged that there is obviously a case for enabling employees of telecommunications providers who do come across information in the course their employment which they consider relevant to security or law enforcement to report that to an appropriate authority. The Report concluded, however, that from a privacy perspective the provisions as presently drafted are inadequate. It was recommended that they be reviewed with a view to clarifying the objective and better identifying the process to be followed.[74]

63.54 On 14 June 2007, the Telecommunications (Interception and Access) Amendment Bill 2007 was introduced into the Australian Parliament House of Representatives. The Bill implements a number of the recommendations of the Blunn Report.[75] The Bill seeks to introduce a new Chapter 4 into the *Telecommunications (Interception and Access) Act* and will transfer ss 282 and 283 of the *Telecommunications Act* to the *Telecommunications (Interception and Access) Act*. In contrast to Part 13 of the *Telecommunications Act*, the proposed Chapter 4 deals with permitted access to 'telecommunications data'. The Bill does not set out a definition of 'telecommunications data'. The proposed s 172 provides that the provisions in Chapter 4 do not permit the disclosure of the 'contents or substance of a communication'. Subject to this limitation, Chapter 4, like the exceptions under Part 13, will authorise access to 'information or a document'.[76]

63.55 Chapter 4 of the Act will establish a two tier access regime for particular officers of ASIO or an enforcement agency to authorise lawfully the disclosure of telecommunications data without breaching the general prohibitions on the disclosure of information or documents under ss 276, 277 and 278 of the *Telecommunications Act*. The first tier allows access to existing telecommunications data.[77] The second tier, which is limited to a narrower range of agencies and requires a higher threshold of authorisation, allows for access to future telecommunications data.[78] Proposed sections 174 and 177 deal with voluntary disclosures of telecommunications data. Requests from agencies for telecommunications data are dealt with under ss 175, 176 and 178–180.

---

73 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, [1.7.6].

74 Ibid, [1.7.6].

75 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 1.

76 See, eg, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) sch 1, proposed s 175.

77 Ibid sch 1, proposed ss 175, 178, 179.

78 Ibid sch 1, proposed ss 176, 180.

63.56 The Bill contains a number of safeguards in relation to access to telecommunications data. For example, authorisations must be retained for a period of three years.[79] The head of an enforcement agency must report the number of authorisations to the Attorney-General of Australia on an annual basis, and this report must be tabled in Parliament.[80] A new s 306A, based on s 306 of the *Telecommunications Act*, provides for records of prospective authorisations made under the *Telecommunications (Interception and Access) Act* to be kept by carriers, carriage service providers and number-database operators.

63.57 On 21 June 2007, the Senate referred the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 to the Legal and Constitutional Affairs Committee for inquiry and report (Senate Committee Inquiry). Submissions to the Senate Committee Inquiry raised a range of privacy issues including:

- The meaning of telecommunications data—the Australian Privacy Foundation and Electronic Frontiers Australia expressed concern about potential access to information about web browsing and chat room sessions, and that the distinction between the content or substance of a message and other data was particularly unclear in relation to email header data.[81]

- Access to prospective telecommunications data—it was suggested in some submissions that the controls over access to prospective telecommunications data do not go far enough. For example, the Law Council of Australia and Electronic Frontiers Australia submitted that access to prospective mobile telephone data should be subject to more stringent control than authorisation by ASIO officers or officers of a criminal law enforcement agency.[82]

- Secondary disclosure provisions—the Police Federation of Australia held concerns regarding how the secondary disclosure provisions might impact on the privacy of police officers, especially those involved in disciplinary proceedings. The NSW Ombudsman, however, argued that the restrictions on secondary disclosure are too narrow.[83]

- Consideration of privacy implications—proposed s 180(5) requires an authorised officer to have regard to likely interference with the privacy of individuals when authorising access to prospective telecommunications data. Submissions from a number of stakeholders, including the OPC, suggested

79 Ibid sch 1, proposed s 185.
80 Ibid sch 1, proposed s 186.
81 Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), [3.11]–[3.16].
82 Ibid, [3.22]–[3.25].
83 Ibid, [3.28]–[3.31].

providing greater guidance on how the privacy implications of an authorisation should be considered and documented.[84]

- Destruction of data—the OPC submitted that proposed ss 174 and 177 should include positive obligations on law enforcement agencies to destroy in a timely manner irrelevant material containing personal information and information which is no longer needed.[85]

- Oversight—the Inspector-General of Intelligence and Security submitted that there may be a role for his office in monitoring authorisations by ASIO officers to access prospective telecommunications data.[86]

63.58 The Senate Committee Inquiry released its report on 1 August 2007. The Committee recommended that the Telecommunications (Interception and Access) Amendment Bill be passed, subject to a number of recommendations. These recommendations included that the:

- Inspector-General of Intelligence and Security incorporate into his regular inspection program oversight of the use of powers to obtain prospective telecommunications data by ASIO;[87] and

- Attorney-General's Department arrange for an independent review of the operation of the *Telecommunications (Interception and Access) Act* within five years.[88]

63.59 Attached to the Committee's report is the minority report by the Australian Democrats.[89] The Australian Democrats conclude that the Bill 'confirms privacy as a valued norm but does not do enough to protect Australians' private conversations and communications'.[90] The report includes five recommendations that differ from the findings of the Senate Committee Inquiry. The Democrats recommend:

- clear language outlining whether or not specific technologies qualify as 'telecommunications data';

- clear language specifying that 'real time data, in other words location information, can only be accessed by enforcement agencies with a warrant', as opposed to access by intra-agency written authorisation;

---

84 Ibid, [3.34]–[3.37].
85 Ibid, [3.39].
86 Ibid, [3.66].
87 Ibid, rec 3.
88 Ibid, rec 4.
89 Ibid, Minority Report by the Australian Democrats.
90 Ibid, Minority Report by the Australian Democrats, [1.40].

- access to mobile telephone location information is limited to fourteen days, non-renewable unless relevant information is gathered from the source within the original fourteen day period, and then only for an additional twenty days;

- a requirement that enforcement agencies consult with the Public Interest Monitor before they apply for an authorisation under the Act;[91] and

- a positive obligation on law enforcement agencies and ASIO to warn communication carriers' employees that they are not legally obliged to make 'voluntary disclosures'.[92]

ALRC's view

63.60 The ALRC agrees with the findings of the Blunn Report and the Senate Committee Inquiry that the exceptions in ss 282 and 283 of the *Telecommunications Act* are better located in the *Telecommunications (Interception and Access) Act*. To this extent, the ALRC supports the transfer of those provisions under the Telecommunications (Interception and Access) Amendment Bill 2007. In light of the recent Senate Committee Inquiry, the ALRC does not propose to conduct another detailed study of the Bill. The ALRC does, however, share a number of the concerns raised in submissions to the Senate Committee Inquiry, including those relating to the destruction of irrelevant material containing personal information, and the need for further oversight of ASIO's powers to obtain prospective telecommunications data.

Question 63–2 Does the Telecommunications (Interception and Access) Amendment Bill 2007 provide adequate protection of personal information that is used or disclosed for law enforcement purposes? For example, should the Bill be amended to:

(a) define 'telecommunications data';

(b) provide greater guidance on how the privacy implications of an authorisation should be considered and documented under proposed s 180(5);

(c) include positive obligations on law enforcement agencies to destroy in a timely manner irrelevant material containing personal information and information which is no longer needed; and

91 The role of a 'Public Interest Monitor' is discussed in Ch 64.

92 Parliament of Australia—Senate Legal and Constitutional Affairs Committee, *Telecommunications (Interception and Access) Amendment Bill 2007* (2007), Minority Report by the Australian Democrats.

(d) provide that the Inspector-General of Intelligence and Security monitor the use of powers by the Australian Security Intelligence Organisation to obtain prospective telecommunications data?

Threat to person's life or health

63.61 Sections 287 and 300 of the *Telecommunications Act* provides that a primary or secondary use or disclosure of information is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person, and the first person believes on reasonable grounds that the use or disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person. ACMA has reported that 4,085 disclosures were made under this exception in 2005–06.[93]

63.62 The guidance notes to the deregistered ACIF *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* stated that this provision is aimed at emergency situations.

> A threat to life or health would be interpreted to include threats to safety—bush fires, industrial accidents etc. Health would include mental as well as physical health, although appeals to the threat of stress or anxiety would not generally be sufficient. The rules require the threat is serious and imminent.[94]

63.63 NPP 2 contains a similar exception. It allows an organisation to use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection if the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety.

63.64 In Chapter 22, the ALRC notes that a large number of stakeholders are of the view that this exception is too narrow. There is considerable concern that the requirement that the threat must be both serious *and* imminent is too difficult to satisfy and that it can lead to personal information not being used or disclosed in appropriate circumstances.

63.65 The ALRC proposes that the exception should apply where the relevant threat is serious, but not necessarily imminent.[95] This approach would allow an agency or

---

93 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145. In 2004–05, there were 885,466 disclosures—an increase of 26% from the previous financial year: Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 186.

94 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 23. Rules 6.1(d) and 7.1(c) of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) provided for a similar exception.

95 Proposal 22–3.

organisation to take preventative action to stop a threat from developing to a point where the danger is likely to eventuate. The ALRC believes that this formulation strikes an appropriate balance between respecting the privacy rights of an individual and the public interest in averting threats to people's life, health and safety.

63.66 In the ALRC's view, the same considerations apply to the exception under the *Telecommunications Act*. The ALRC therefore proposes that the exception under ss 287 and 300 of the *Telecommunications Act* provide that a use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to a person's life, health or safety; or public health or public safety.

Proposal 63–3 Sections 287 and 300 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a person of information or a document is permitted if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

  (i) a person's life, health or safety; or

  (ii) public health or public safety.

Knowledge of person concerned

63.67 Section 289(1)(b)(i) of the *Telecommunications Act* provides that the use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person, and the other person is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned.

63.68 ACMA has reported that disclosures made under s 289 rose sharply from 75,422 in 2004–05 to 133,765 in 2005–06 (a 77% increase). ACMA has stated that this increase can be explained in part by carriers disclosing customer details for credit-worthiness checks.[96]

96 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 145.

63.69 NPP 2.1(a) contains a similar exception where an individual would reasonably expect an organisation to use or disclose the information for a purpose (the secondary purpose)[97] other than the primary purpose of collection. NPP 2, however, contains the added protection that the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection.

Submissions and consultations

63.70 Electronic Frontiers Australia noted that s 289 and NPP 2.1(a) offer very different levels of protection:

> In the case of use or disclosure for the primary purpose of collection, the *Telecommunications Act* (s 289) is more protective than the *Privacy Act* (NPP 2). The TA restricts use or disclosure for the primary purpose to circumstances of which the individual is 'reasonably likely to have been aware' or has consented. In contrast, NPP 2 does not restrict use or disclosure for the primary purpose at all.
>
> However, in the case of use or disclosure for a secondary purpose of collection, the *Telecommunications Act* is significantly less protective than the *Privacy Act*. NPP 2.1 prohibits use or disclosure unless both 'the secondary purpose is related to the primary purpose of collection' (and directly related if sensitive information) and 'the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose' (or has consented).[98]

63.71 Electronic Frontiers Australia submitted that either the *Privacy Act* or *Telecommunications Act* must be amended to require businesses in the telecommunications sector to comply with NPP 2.1(a) in relation to use and disclosure for secondary purposes. Electronic Frontiers Australia also noted that the existing protection under s 289 in relation to use and disclosure for the primary purpose must not be removed or made any weaker.[99] The OPC noted that this exception appears to be more permissive than NPP 2, and it was concerned that this exception may lower the threshold of privacy protection in the telecommunications sector.[100]

ALRC's view

63.72 In Chapter 22, the ALRC considers various reformulations of the reasonable expectation exception, but suggests that the exception under NPP 2 provides the appropriate level of protection for an individual's personal information. The term 'reasonable expectation' imports an objective test of what a hypothetical reasonable individual would expect in the relevant circumstances. The ALRC notes that this condition is an important, but not particularly onerous, protection against the misuse of an individual's personal information.

---

97 According to the OPC, this means that 'the secondary purpose must be something that arises in the context of the primary purpose': Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

98 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

99 Ibid.

100 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

63.73 The ALRC also believes that the requirement that the secondary purpose is related to the primary purpose of collection (and, if the personal information is sensitive information, directly related to the primary purpose of collection) is appropriate in the telecommunications context. An individual is more likely reasonably to expect the use or disclosure of their personal information if the use or disclosure is related, or in the case of sensitive information directly related, to the primary purpose of collection.

Proposal 63–4 Section 289 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a person of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(a) the other person has consented to the use or disclosure; or

(b) if the use or disclosure is for a purpose other than the primary purpose for which the information was collected (the secondary purpose):

  (i) the secondary purpose is related to the primary purpose and, if the information or document is sensitive information (within the meaning of the *Privacy Act 1988* (Cth)), the secondary purpose is directly related to the primary purpose of collection; and

  (ii) the other person would reasonably expect the person to use or disclose the information.

Consent

63.74 Section 289(1)(b)(ii) provides that the use or disclosure by a person of information is permitted if the information relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person and the other person has consented to the use or disclosure. Consent is also an exception under NPP 2.1(b) and the proposed 'Use and Disclosure' principle.[101]

63.75 The *Telecommunications Act* does not provide a definition of 'consent' for the purposes of s 289 or other provisions.[102] Section 6 of the *Privacy Act* defines 'consent' as 'express consent or implied consent'. Although s 290 of the *Telecommunications Act* suggests that consent may be express or implied, this is not stated expressly. In the interest of clarity, and consistency with the *Privacy Act*, the ALRC proposes that

101 See also Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999) rr 6.1(b), 7.1(b).

102 See discussion of s 290 below.

Part 13 of the *Telecommunications Act* should be amended to provide that 'consent' means 'express consent or implied consent'.

63.76 In Chapter 16, the ALRC considers various options for reform of the definition of consent. In the ALRC's view, however, the specific requirements of consent—particularly as regards the requisite level of voluntariness—are highly dependent on the context in which the personal information is collected, used or disclosed. In other words, what may be required to obtain valid consent in one situation may differ, sometimes significantly, from what is required to obtain consent in another situation.

63.77 In the ALRC's view, the OPC should provide further guidance on the meaning of consent. In Chapter 64, the ALRC proposes that the OPC, in consultation with ACMA, Communications Alliance and the TIO, should develop and publish guidance relating to privacy in the telecommunications industry. This guidance should explain how consent may be obtained in certain contexts that are of particular importance—such as, when an individual is entering an agreement for the provision of services with a telecommunications provider. This guidance should also include advice on when it is appropriate to use the mechanism of bundled consent.

Proposal 63–5 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that 'consent' means 'express or implied consent'.

Implicit consent

63.78 Section 290 of the *Telecommunications Act* provides that the use or disclosure by a person of information is permitted if the information relates to the contents of a communication made by another person, and having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented if they had been aware of the use or disclosure.[103] The Explanatory Memorandum to the Telecommunications Bill 1996 (Cth) states that this exception is intended to allow disclosure of public communications, for example, where a carrier discusses the content of an online bulletin board, or the content of a pay-television program carried on a cable network.[104]

63.79 The OPC noted that this exception appears to be more permissive than NPP 2, and it was concerned that this exception may lower the threshold of privacy protection in the telecommunications sector.[105] Electronic Frontiers Australia stated that the scope of the exception is unclear and does not protect adequately personal information of third parties referred to in a communication. Electronic Frontiers Australia submitted

103 *Telecommunications Act 1997* (Cth) s 306(1).

104 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 10. See also Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 21.

105 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

that s 290 should be amended to ensure that personal information about third parties cannot be disclosed based on an assumption that the sender and recipient would have consented.[106]

63.80 The ALRC agrees that the intent of s 290, as expressed in the Explanatory Memorandum to the Telecommunications Bill 1996, is not reflected clearly in the wording of the section. It is the ALRC's preliminary view that the provision should be amended to clarify that it relates only to public communications. Prior to making a proposal, the ALRC is interested in stakeholder's views on how the provision could be clarified.

Question 63–3 How does s 290 of the *Telecommunications Act 1997* (Cth) operate in practice? Is the exception resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined?

Business needs of other carriers or service providers

63.81 Sections 291 and 302 of the *Telecommunications Act* provide that the primary and secondary use or disclosure by a person of information is permitted if: it is made by or on behalf of a carrier or carriage service provider for the purposes of facilitating another carrier or service provider providing a service to the person who is the subject of the information or document; and that person has been or is a customer of the disclosing carrier or carriage service provider or the other carrier or service provider.

63.82 The provision also contains rules that allow the use or disclosure of information or a document about customers for a purpose connected with a carriage service intermediary arranging the supply of a carriage service by a carriage service provider to a third person.[107]

63.83 This provision is designed to allow uses and disclosures that are 'triggered' by some action or request by a customer such as dialling an access code to make use of another carrier. It does not provide for uses and disclosures of subscriber information for speculative activity such as marketing by other carriers or service providers.[108]

63.84 Submissions raised a number of issues in relation to this exception. These issues related to the scope of the exception and whether it permitted the use and disclosure of silent numbers, calling number display or location-based information.[109] Submissions also raised concerns that telecommunications providers have interpreted s 291 and

106 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
107 Explanatory Memorandum, Telecommunications Bill 1996 (Cth), vol 2, 10–11.
108 Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999), 20–21.
109 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

other provisions under Part 13 to allow the use or disclosure of credit reporting information and credit worthiness information.

Silent numbers and calling number display

63.85 Electronic Frontiers Australia submitted that, since 21 December 2001 when the private sector provisions commenced and the ACIF *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers* was deregistered, a number of telecommunications providers have been disclosing calling line identification (CLI) to some of their internet service provider (ISP) customers. CLI provides these ISPs with caller identification information regardless of whether permanent or per call blocking has been enabled on these lines. That is, the default blocking of calling number display (CND) for unlisted numbers and caller initiated blocking of CND are not operative by virtue of the arrangement of these carriers.

63.86 Electronic Frontiers Australia noted that it had made a complaint to the Australian Communications Authority (ACA) (now ACMA) and the OPC about this issue.[110] Both the ACA and the OPC found that this use and disclosure was permitted under s 291 of the *Telecommunications Act*. Electronic Frontiers Australia submitted that telecommunications service providers are relying on s 291 to use and disclose personal information in circumstances that would otherwise be in breach of NPP 2. It was submitted that this is contrary to previous interpretations of s 291 made publicly available by the ACA and TIO. For example, the Australian Communications Authority manual *Telecommunications and Law Enforcement* states that this exception would permit a carriage service intermediary to pass on the details of a customer to a network operator so as to permit connection. Disclosures would also be permitted where a customer changes his or her carriage service provider.[111]

63.87 The TIO *Position Statement—Customer's Personal Information Passed to Another Provider* currently states:

> Section 291 of Part 13 of the *Telecommunications Act 1997* allows the provider who has the customer's details to disclose the customer's information to another provider so that it can bill for the calls made, even if the customer's telephone service is not with that particular provider. Information can be forwarded in this way even where the number is silent; however, mutual arrangements between companies should prevent silent line information appearing in any directory services.[112]

63.88 Electronic Frontiers Australia submitted that either the *Telecommunications Act* or the *Privacy Act* should be amended so that all businesses in the telecommunications services industry are required to comply with NPP 1 in relation to necessary collection and NPP 2 in relation to use and disclosure. This would mean that ss 291 and 302 could not be interpreted or applied in a way that is inconsistent with the *Privacy Act*. It

---

110 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

111 Australian Communications Authority, *Telecommunications and Law Enforcement* (1998), 22.

112 Telecommunications Industry Ombudsman, *Position Statement—Customer's Personal Information Passed to Another Provider* <www.tio.com.au> at 2 August 2007.

was submitted that compliance with the NPPs would not prevent service providers collecting, using and disclosing information for necessary purposes, such as those stated by the ACA and TIO above.[113]

63.89 The ALRC notes that the scope of ss 291 and 302 is unclear. Although NPP 2 would allow a use and disclosure for the purpose of s 291 because it would be 'required or authorised by or under law', there is no equivalent to s 291 under NPP 2. It could be argued that it lowers the level of protection offered under the *Privacy Act*. In the ALRC's view, the scope of the exception should be clarified.

63.90 One option would be to amend ss 291 and 302 to confine the exception to certain duties of an employee or contractor, including connecting and disconnecting telecommunications services, and limit expressly the circumstances when silent and other blocked calling numbers can be used or disclosed. Another option would be to subject the exception to a requirement that a use and disclosure by a person made for the purpose of performing that person's duties must be related to the primary purpose of collection. The ALRC is interested in stakeholder views on whether it is practical to limit this exception in this way.

Question 63–4 Is the exception that permits the use or disclosure of information or a document for certain business needs of other carriers or service providers (s 291 and s 302 of the *Telecommunications Act 1997* (Cth)) resulting in the inappropriate use or disclosure of personal information? If so, how should the exception be confined? Should the exception be amended to provide that silent and other blocked calling numbers can only be used or disclosed with a person's consent?

Location-based services

63.91 Electronic Frontiers Australia submitted that it is not clear whether s 291 of the *Telecommunications Act* provides adequate protection of location-based information.[114] Location-based services have been used for some time. For example, certain numbers starting with '13' (such as those used by taxi services or food delivery chains) involve the use of location-based technology. 'Triple 0' emergency calls also capture location information. There are a range of commercially offered location-based services. These are broadly divided into two categories:

- 'active' or 'pull' services that are initiated by an action, such as an SMS, from the consumer requesting that a taxi be sent to the person's present location; and

113 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
114 Ibid.

- 'passive' or 'push' services that are not requested by the consumer. These may take the form of marketing distributed to consumers according to their whereabouts, or they may take the form of 'tracking' services initiated by third parties interested in the location of other consumers. Passive location-based services are not currently offered in Australia.[115]

63.92 DCITA considered location-based services in its review of the regulation of content delivered over convergent devices.[116] It noted that the use of active location-based services is likely to be taken as constituting informed consent. The review was concerned, however, that passive location-based services could be misused for illegal or inappropriate purposes if offered without appropriate safeguards.[117]

63.93 DCITA noted that s 291 of the *Telecommunications Act* may operate in certain circumstances to allow for the use and disclosure of location information without a user's consent or knowledge. DCITA found that this application of s 291 suggests that an alternative means of protecting against the privacy and safety issues associated with passive services should be pursued. The review found that it would be appropriate to require the consent of an account holder prior to the use or disclosure of location information relating to any handsets operated under an account.[118] It was noted that this approach was consistent with the requirements under the EU *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*.[119]

63.94 The *Communications Legislation Amendment (Content Services) Act 2007* (Cth) will implement the DCITA recommendations. This Act will amend s 291 to provide that the use or disclosure by a person of information or a document is permitted if the information or document relates to the location of a mobile telephone handset or any other mobile communications device, and the person has consented to the disclosure, or use. The Act is due to commence on 20 January 2008.[120]

Credit reporting information and credit worthiness

63.95 Concerns were raised in a number of submissions about whether Part 13 of the *Telecommunications Act* permitted the use and disclosure of credit information and

---

115 Australian Government Department of Communications Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006).

116 Ibid, 31–32.

117 Ibid, 102.

118 Ibid, 104–105.

119 Ibid, 105. See European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002), arts 6–9. While this approach would provide sufficient safeguards to prevent abuse of passive location-based services with respect to adults, DCITA concluded that further measures will be required where services are offered that would identify the location of minors: Australian Government Department of Communications Information Technology and the Arts, *Review of the Regulation of Content Delivered Over Convergent Devices* (2006), 104–105. Communications Alliance also considered privacy issues related to location-based services: Communications Alliance Ltd, *Submission PR 198,* 16 February 2007.

120 *Communications Legislation Amendment (Content Services) Act 2007* (Cth) sch 1, pt 1.

credit worthiness information that would otherwise not be permitted under the *Privacy Act*.

63.96 Telstra noted that a number of provisions in the *Privacy Act* prohibit disclosure of credit information except where disclosure 'is required or authorised by or under law'.[121] In Telstra's view, a disclosure which falls within one of the exceptions in Part 13 of the *Telecommunications Act* will be 'authorised by law' under Part IIIA and the NPPs in the *Privacy Act*.

63.97 The OPC expressed concern that the exceptions under ss 289, 290 and 291 of the *Telecommunications Act* appear to permit additional uses and disclosures in relation to consumer credit.[122] The OPC noted that ACMA has published advice on its website stating that ss 289 and 290 may permit the disclosure of affairs or personal particulars of another person in relation to a debt sold to a debt collection agency or when a carrier or carriage service provider does credit card checks with a credit card company.[123] The OPC submitted that this interpretation of ss 289 and 290 creates two problems.

> First, these exceptions appear to go beyond what a credit provider is permitted to do under the credit reporting provisions in Part IIIA of the *Privacy Act*. However, because of s 303B of the *Telecommunications Act* … such uses and disclosures are taken to be authorised by law for the purposes of the *Privacy Act*, when undertaken by telecommunications businesses covered by Part 13.
>
> Second, sections 289 and 290 appear to create more permissive conditions for use and disclosure of personal information related to consumer credit for those credit providers that operate in the telecommunications sector, compared to those that operate in other industries.[124]

ALRC's view

63.98 In the ALRC's view, Part 13 of the *Telecommunications Act* should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the *Privacy Act.*[125] Adverse personal credit listings can have a significant impact on the life and opportunities of an individual. As outlined in Part G, the ALRC believes that credit reporting information requires a specific level of detail to ensure that credit providers, credit reporting agencies and individuals understand their obligations and rights. This information should not be regulated under general provisions such as ss 289, 290 and 291 of the *Telecommunications Act*. There

---

121 *Privacy Act 1988* (Cth) ss 18Q(3), 18Q(5), 18N(1)(g).

122 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

123 Australian Communications and Media Authority, *Disclosure of Customer Details under Part 13 of the Telecommunications Act 1997 FAQs* <www.acma.gov> at 15 August 2007.

124 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

125 See Ch 50 for a discussion of 'credit reporting information' and information about the credit worthiness of another person. In that chapter, the ALRC proposes that the proposed *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.

is no reason why organisations in the telecommunications industry should be subject to more permissive credit reporting rules than organisations in other industries.

Proposal 63–6 Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that use or disclosure by a person credit reporting information is to be handled in accordance with the *Privacy Act*.

Integrated public number database

63.99 Currently, Telstra's carrier licence requires it to provide and maintain an 'integrated public number database' (IPND).[126] The IPND, which was established in 1998, is a database of all listed and unlisted telephone numbers and associated customer data—namely, the name and address of the customer, the customer's service location, the name of the carriage service provider, and whether the telephone is to be used for government, business, charitable or private purposes.[127]

63.100 Section 472(1) of the *Telecommunications Act* allows the Minister (currently the Minister for Communications, Information Technology and the Arts)[128] to determine that a person other than Telstra should provide and maintain an IPND. Any such determination has no effect while Telstra's carrier licence requires it to provide and maintain an IPND,[129] however, and to date, no such determination has been made.

63.101 The *Telecommunications Act* requires carriage service providers to provide Telstra with as much information as is reasonably required to provide and maintain the IPND.[130] Accordingly, disclosure of telecommunications information for inclusion in the IPND is not an offence under Part 13 of the Act because it is 'required or authorised by or under law'.[131]

63.102 Telstra reported that the IPND contained 45,999,620 connected records at 30 June 2006, an increase of 2,413,787 records (or 9.5%) over the previous 12 month period. At 30 June 2006, 31 carriers and carriage service providers were listed as data providers to the IPND, compared with 24 in the previous 12 month period.[132]

---

126 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.
127 Ibid, cl 10(4).
128 Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007], sch pt 3.
129 *Telecommunications Act 1997* (Cth) s 472(5).
130 Ibid s 101, sch 2 pt 4.
131 Ibid s 280.
132 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 147. At 30 June 2005, 24 carriage service providers provided data to the IPND and the IPND contained approximately 43.6 million records: Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 184.

63.103 Telstra's carrier licence limits the purposes for which information in the IPND can be used and disclosed.[133] It can only be disclosed to a carriage service provider to enable the provider to: provide directory assistance, operator assistance or operator services; produce a public number directory; provide location dependent carriage services; or assist emergency call services and enforcement agencies.[134]

63.104 Telstra's carrier licence also provides that access to information in the IPND is subject to Part 13 of the *Telecommunications Act*.[135] Section 285 of the Act allows use or disclosure of IPND information about the affairs or personal particulars of a person for purposes connected with the: provision of directory assistance services by or on behalf of a carriage service provider; publication or maintenance of a directory of public numbers; or matter raised by a call to an emergency service number.

63.105 Where the *Privacy Act* applies to a person who discloses or uses IPND information, the disclosure or use of such information will not breach the *Privacy Act* so long as the disclosure or use occurs in accordance with sections 285 and 299A of the *Telecommunications Act*. That is, the disclosure or use will be authorised by law for the purposes of the *Privacy Act*.[136]

63.106 In November 2003, the ACA announced its intention to develop an industry standard to articulate clearly the uses that may be made of information provided by customers to telecommunications providers. It stated that an industry standard was required because investigations had revealed that information in the IPND was being used for purposes other than those envisaged by Part 13 of the *Telecommunications Act*. These purposes included 'database enhancement', 'data cleansing', 'data verification', and 'list management'.[137]

63.107 In March 2004, the ACA released a discussion paper on regulating the use of IPND data.[138] In May 2005, it released a draft industry standard on the use of IPND data.[139] Had the draft standard been implemented, it would have applied to the 'public number data' section of the telecommunications industry.[140] It would have regulated further the use of IPND data; ensured that customers were aware of the purposes of the collection of IPND data and the purposes for which the information may be disclosed; and enabled customers to choose whether to include their data in a public number directory.

---

133 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 10(7).
134 Ibid, cl 10(1).
135 Ibid, cl 10(9)(b).
136 *Telecommunications Act 1997* (Cth) s 303B.
137 Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 11.
138 Ibid.
139 Australian Communications Authority, *Draft Telecommunications (Use of Integrated Public Number Database) Standard* (2005).
140 This would be determined pursuant to s 110 of the *Telecommunications Act 1997* (Cth).

63.108 In December 2006, however, the Australian Parliament passed the *Telecommunications Amendment (Integrated Public Number Database) Act 2006* (IPND Act). The IPND Act introduced a definition of 'public number directory' into the *Telecommunications Act* in order to prevent IPND data being used directly for unauthorised purposes, such as the development of reverse search directories, and the production of databases which are used for purposes such as marketing, data cleansing and appending, debt collection, identity verification and credit checking.[141] It is unlikely that consumers of telecommunications services would be aware of, or to have consented to, the use of their personal information for purposes beyond the existing public interest uses permitted by the *Telecommunications Act*, such as emergency services and law enforcement.[142] Arguably, therefore, such uses are problematic from a privacy perspective.

63.109 The IPND Act also introduced a new exception to the offence provisions under the *Telecommunications Act* that allows IPND information to be disclosed for specified research purposes that are in the public interest. ACMA have promulgated a *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* that sets out the kinds of research that will be considered to be in the public interest. The public interest research exception is discussed further below.

63.110 Under former arrangements Telstra, as the IPND Manager, was responsible for deciding applications for access to the IPND for all users. The IPND Act amended the *Telecommunications Act* to provide that IPND data users are required to apply to ACMA for an authorisation to access the IPND. Telstra will only be permitted to disclose IPND data to persons holding such an authorisation.

63.111 The IPND Act also requires ACMA to establish a scheme for the granting of authorisations permitting persons to use and disclose IPND information.[143] The Act requires ACMA to consult with the Privacy Commissioner and Attorney-General's Department on development of the scheme.[144] Criminal sanctions apply for unauthorised secondary disclosure and use of IPND data by public number directory publishers, and for breaches of conditions of authorisations issued under the IPND scheme.[145] ACMA has established an IPND Scheme under the *Telecommunications Integrated Public Number Database Scheme 2007* and a number of other instruments.[146]

---

141 Ibid s 285(2).

142 Explanatory Memorandum, Telecommunications Amendment (Integrated Public Number Database) Bill 2006 (Cth), 2.

143 *Telecommunications Act 1997* (Cth) s 295A.

144 Ibid s 295M.

145 Ibid pt 13 div 3A.

146 Including the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* and the *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)*. These instruments are discussed further below.

Should the IPND be regulated under the Privacy Act?

63.112 One issue for consideration in this Inquiry is whether the IPND should be regulated under the *Privacy Act* rather than the *Telecommunications Act*.

63.113 DCITA submitted that, if only the NPPs were relied upon to govern use and disclosure of IPND information, the NPPs may prevent the disclosure and use of IPND information for purposes which are currently permitted under the *Telecommunications Act*. These purposes, DCITA argues, continue to be important for the effective operation of the telecommunications industry, and for public safety reasons.[147]

63.114 DCITA also submitted that NPP 2 provides that personal information that is not sensitive information can be used or disclosed for the secondary purpose of direct marketing if certain criteria are met. DCITA submitted that IPND information is not currently permitted to be used for direct marketing purposes and expressed the view that this should continue to be the case.[148]

ALRC's view

63.115 Although many of the issues raised by DCITA could be accommodated by amendments to the *Privacy Act*, the ALRC considers that the IPND should continue to be regulated under Part 13 of the *Telecommunications Act*. The IPND is an up-to-date, comprehensive database containing the details of all listed and unlisted telecommunications subscribers. The special nature of the IPND means that a high standard of protection should apply.

63.116 Further, personal information held on the IPND is required to be collected by law, but disclosed and used for purposes not always related to the purpose for which the information was collected. The Australian community is entitled to expect a high level of control over access to that information, and the purposes for which it may be accessed, used and disclosed. In the ALRC's view, the current legislative regime relating to the IPND under the *Telecommunications Act* provides adequate protection of information held under the IPND.

Research exception

63.117 Sections 285(1A)(c)(iv) and 285(1A)(d) of the *Telecommunications Act* provide an exception to the prohibition on use and disclosure of information contained in the IPND. If the disclosure is made to another person for purposes connected with the conduct of research of a kind specified in an instrument under s 285(3), and the other person has been authorised by ACMA to use and disclose the information, such access is permitted. Section 285(3) provides that the Minister may, by legislative instrument, specify kinds of research that are in the public interest.

---

147 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

148 Ibid.

63.118 On 4 May 2007, the Minister for Communications, Information Technology, and the Arts issued the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)*. The Instrument sets out permitted research for the purposes of the s 285(1A)(c)(iv) exception:

- research, or the compilation or analysis of statistics, relevant to public health, including epidemiological research, where the research is not conducted for a primarily commercial purpose;

- research regarding an electoral matter conducted by a registered political party, a political representative, a candidate in an election for a Parliament or a local government authority or a person on behalf of such a party, representative or candidate, where the research is not conducted for a primarily commercial purpose; and

- research conducted by or on behalf of the Commonwealth, a Commonwealth authority or a prescribed FMA agency which will contribute to the development of public policy, where the research is not conducted for a primarily commercial purpose.[149]

63.119 The OPC submitted that the research exception may be interpreted too broadly. The OPC believes that particular terms should be defined in the Act itself, such as what constitutes research in the public interest and, in terms of medical research, what would be considered 'non-commercial use'.[150]

63.120 A key concept in each of these categories is that the research 'is not conducted for a primarily commercial purpose'. This is in contrast to the National Health and Medical Research Council guidelines made under ss 95 and 95A of the *Privacy Act*.[151] These guidelines provide that where research may breach the IPPs or NPPs, the research must be approved by a Human Research Ethics Committee (HREC). Before approving a particular research proposal under the guidelines, HRECs are required to consider whether the public interest in the research *substantially outweighs* the public interest in the protection of privacy.[152]

---

149 *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)*. A 'prescribed FMA agency' is a body, organisation or group mentioned in the *Financial Management and Accountability Regulations 1997* (Cth) sch 1.

150 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

151 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000); National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

152 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000), Guideline 3.2; National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001), Guideline D.4.

63.121 In Chapter 58, the ALRC proposes that the test under the s 95 and 95A guidelines be amended to provide that, before approving an activity, a HREC must be satisfied that the public interest in the activity *outweighs* the public interest in maintaining the level of privacy protection provided by the proposed Unified Privacy Principles (UPPs).

63.122 In the ALRC's view, when considering whether IPND information should be made available for research purposes, consideration of whether a research project is for a commercial purpose is not the correct test. It will not always be clear when research is primarily conducted for a commercial purpose. Further, research that is clearly in the public interest may also have a commercial purpose. In the ALRC's view, the appropriate test is whether the public interest in the relevant research outweighs the public interest in maintaining the protection of the personal information held on the IPND.

Proposal 63–7 The Australian Government should amend the *Telecommunications (Integrated Public Number Database—Permitted Research Purposes) Instrument 2007 (No 1)* to provide that the test of research in the public interest is met when the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.

Notifying the Privacy Commissioner of a breach

63.123 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* sets out the conditions upon which ACMA may grant authorisations for access to personal information contained in the IPND under the IPND scheme.

63.124 Clause 6 of the Determination provides that an authorisation under the IPND scheme is subject to a condition requiring the holder of the authorisation, as soon as practicable after the holder becomes aware of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information, to notify ACMA and the IPND Manager, and to take reasonable steps to minimise the effects of the breach.

63.125 In the ALRC's view, the holder of an authorisation should also be required to notify the OPC as soon as practicable after the holder becomes aware of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information. It is important

that the OPC be given an opportunity to investigate whether a breach of security has also resulted in an interference with an individual's privacy.[153]

Proposal 63–8 The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Office of the Privacy Commissioner, as soon as practicable after becoming aware:

(a) of a substantive or systemic breach of security that could reasonably be regarded as having an adverse impact on the integrity and confidentiality of the protected information; and

(b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.

Public number directories not sourced from the IPND

63.126 The ACA has noted that Telstra's directory arm, Sensis, has a database of information provided to it by other telecommunications providers under bilateral agreements. This enables Sensis to publish the White Pages based on this information, rather than from information sourced from the IPND.[154] Consequently, Sensis is not subject to the IPND provisions under the *Telecommunications Act* because it sources the information for its directories directly from telecommunications companies and not from the IPND.

Submissions and consultations

63.127 In IP 31, the ALRC noted that it was interested in hearing whether current uses of personal information by producers of public number directories are appropriate and whether there should be any further protections on the use of such information.[155]

63.128 Concern was expressed in submissions that publishers of public number directories that do not use the IPND are not adequately regulated. ACMA noted that this was a key concern highlighted in submissions to ACMA's Telecommunications

153 In Chapter 47, the ALRC proposes that the *Privacy Act* should be amended to include a new Part on data breach notification, which will provide that an agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual. See Proposal 47–1.

154 Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 8.

155 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), [10.33].

(Use of Integrated Public Number Database) Draft Industry Standard 2005.[156] It was noted that the IPND Act amendments to the *Telecommunications Act* will not affect publishers of public number directories that do not use the IPND.[157] A number of stakeholders suggested that directory publishers should be subject to the same regulatory standards, irrespective of the source of the data.[158]

63.129 It was also submitted that the current regulatory scheme results in an 'uneven playing field' and huge gaps in the protection of personal information.[159] In particular, it was noted that there is no prohibition on directory publishers producing directories which are not sourced from the IPND that are reverse-searchable.[160] ACMA noted that it routinely receives complaints from the community about the existence of reverse search directories. ACMA is unable to take action to shut down a reverse search directory where the data comes from another source, or if it cannot establish that IPND customer data is the source used. ACMA gave the following example:

> ACMA has previously investigated two incidences where telephone directories were provided on CD-ROM. In both these cases, ACMA was unable to confirm that information was obtained from a primary disclosure of IPND data, as prohibited by Part 13 of the Tel Act. In one of the cases, it was identified that the likely origin of the data was Sensis' White Pages directory.[161]

63.130 This was confirmed in other submissions to the Inquiry. One member of the public submitted that:

> It is an invasion of privacy that commercial marketers can use reverse telephone directories. I rent a telephone line from Telstra but I have not specifically given them permission to sell my personal information to any organisation, who can on-sell it to goodness knows who, for whatever purpose ... It is not appropriate that private individuals have to opt OUT of contact via these directories. It is appropriate that White Pages be prevented from on-selling information that has been collected for a completely other purpose.[162]

ALRC's view

63.131 There are arguments that directory products that are produced from sources other than the IPND should be subject to Part 13 of the *Telecommunications Act*. In particular, the ALRC notes that the *Telecommunications Act* does not prohibit directory publishers producing reverse-searchable directories which are not sourced from the

---

156 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

157 Ibid; Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007; Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

158 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007; Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

159 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

160 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

161 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

162 S Alexander, *Submission PR 51,* 18 August 2006.

IPND. The ALRC is interested on further stakeholder views on this issue before coming to a final view.

> **Question 63–5** Should directory products that are produced from data sources other than the Integrated Public Number Database be subject to the same rules under Part 13 of the *Telecommunications Act 1997* (Cth) as directory products which are produced from data sourced from the Integrated Public Number Database?

Are public number directories desirable?

63.132 A significant issue for consideration is whether public number directories that contain contact details of residential consumers are still desirable. ACMA submitted that, given the proliferation of mobile phones and the corresponding lack of mobile phone directories, it may be that the community sees decreasing benefit in public number directories. This would especially be the case for non-business users. Many individuals now prefer to limit the provision of their information, rather than have it publicly available.[163]

63.133 A member of the public submitted that:

> We object to the publication of our house number (and street name and suburb) in the Telstra/Sensis 'White Pages Directory' … We are a telephone subscriber, not an address book subscriber and we regard the publication of our address in the above directory as an invasion of our privacy … A serious consequence of Telstra's selling of names, addresses and phone numbers to all and sundry, is the proliferation and onslaught of marketing phone calls one receives at all hours of the day and night. This has to stop and Telstra's authority to sell private details must be revoked, by legislation if necessary.[164]

63.134 The Australian Institute of Mercantile Agents submitted, however, that public number directories should be more readily available.

> The IPND directories must be regarded as allowable public information. This is the only source of locator information our members have access to and yet availability of this data continually is challenged … Our industry is under the constant threat of banning access to information for debt collection purposes. The only persons assisted by such heavy handed misguided intervention are those who do not meet their contractual obligations.[165]

63.135 The ALRC does not have a view on whether public number directories are still desirable. The ALRC notes, however, that it is important that subscribers to telecommunications services are informed that their personal information will be

---

163 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

164 Confidential, *Submission PR 60,* 27 November 2006.

165 Institute of Mercantile Agents, *Submission PR 101,* 15 January 2007. See also Australian Finance Conference, *Submission PR 294,* 18 May 2007.

included in a public directory. One option for consideration is whether the *Telecommunications Act* should be amended to provide that a telecommunications provider is obligated to inform an individual that his or her personal information may be included in a public number directory. The ALRC notes that art 12.1 of the European Union *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* provides that:

> Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.[166]

63.136 The ALRC does not consider that it is necessary expressly to provide for this duty in the *Telecommunications Act*. The ALRC understands that telecommunications providers generally inform their customers that their personal information will be included in a public directory. Further, the telecommunications industry is currently subject to NPP 1.4, which requires an organisation at or before the time it collects personal information from the individual to take reasonable steps to ensure that the individual is aware of the purposes for which the information is collected. The ALRC has proposed that this requirement remain under the proposed 'Specific Notification' principle.

63.137 NPP 5 requires an organisation to set out in a document clearly expressed policies on its management of personal information. The ALRC has proposed that this requirement remain under the proposed 'Openness' principle. These obligations would require a telecommunications supplier to indicate to individuals that their personal information may be included in a public directory.

63.138 Further, in Chapter 64, the ALRC proposes that the OPC, in consultation with ACMA, Communications Alliance and the TIO, should develop and publish guidance relating to privacy in the telecommunications industry. In the ALRC's view, this guidance should address a telecommunication supplier's obligation to inform an individual that their personal information may be included in a public number directory.

Unlisted numbers

63.139 The *Telecommunications Act* provides that an unlisted number cannot be disclosed except in specified contexts.[167] The Act is silent on whether a fee can be charged for an unlisted number. The *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* defines an unlisted number as a public number that is one of the following kinds:

---

166 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).

167 *Telecommunications Act 1997* (Cth) ss 276(1)(a)(iv), 277(1)(a)(ii), 285(1)(a), 285(2).

- a mobile number, unless the customer and the carriage service provider that provides the mobile service to the customer agree that the number will be listed;
- a geographic number that the customer and the carriage service provider that provides services for originating or terminating carriage services to the customer agree will not be included in the directory;
- the number of a public payphone; and
- a number that, when dialled, gives access to a private telephone exchange extension that the customer has requested not be included in the directory.[168]

63.140 The ALRC notes that art 12.2 of the European Union *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* provides that a fee should not be charged for an unlisted number:

> Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.[169]

63.141 ACMA noted that some stakeholders making submissions to it in relation to its Telecommunications (Use of Integrated Public Number Database) Draft Industry Standard 2005 suggested that the imposition of a fee may impact on a consumer's decision to choose to have an unlisted number. Consumers have queried whether such a fee contravenes the *Privacy Act*, and asked why a fee is imposed for an unlisted fixed line number, but not for mobile services.[170]

63.142 In its submission to ACMA on the Telecommunications (Use of Integrated Public Number Database) Draft Industry Standard 2005, the OPC noted that:

> One of the stated objects of the draft standard (clause 5(d)) is that an individual 'may choose whether his or her customer data is to be included in a public number directory'. A relevant question then is whether it is appropriate for individuals to be expected to pay for the right to make privacy choices. Charging a fee for a silent number or to make other choices may limit some individuals' ability to make such choices freely, and thereby hamper their ability to control their own personal information. The effect that free silent listings may have on the number of individuals that appear in directories of public numbers may also need to be considered.[171]

---

168 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* cl 3.

169 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).

170 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

171 Office of the Privacy Commissioner, *Submission to Telecommunications (Use of Integrated Public Number Database) Draft Industry Standard 2005*, August 2005.

63.143 While charging for an unlisted number may not be a breach of NPP 8, it reduces an individual's ability to control the use or disclosure of their personal information. Many people request an unlisted number because of safety concerns or because they do not wish to be contacted by telemarketers.[172] The ALRC proposes, therefore, that the *Telecommunications Act* be amended to prohibit the charging of a fee for an unlisted number in a public number directory.

Proposal 63–9 The *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

Small business exemption

63.144 The *Privacy Act* does not generally apply to businesses with an annual turnover of $3 million or less.[173] Telecommunications providers in this category are, however, obliged to comply with Part 13 of the *Telecommunications Act*. As discussed above, Part 13 only regulates the use and disclosure of information. It does not regulate other aspects of the information-handling cycle, such as the collection and storage of personal information.[174]

63.145 In addition, some organisations that are closely associated with the telecommunications industry may not fall under Part 13 of the *Telecommunications Act* or the *Privacy Act.* For example, organisations other than telecommunications providers can access information from the IPND or collect information from telecommunications providers to produce public number directories. If these organisations have an annual turnover of $3 million or less, they may operate outside all of the existing schemes that regulate privacy in the telecommunications sector.[175]

172 A number of respondents to the ALRC's National Privacy Phone-In on 1–2 June 2006 noted that they had unlisted numbers to avoid telemarketers. See Chapters 1 and 64 for discussion of the National Privacy Phone-In. In relation to the use of unlisted numbers and safety concerns, see Electronic Frontiers Australia, *Privacy Risks of Supply of Blocked Calling Numbers to ISPs* <www.efa.org.au> at 15 August 2007.

173 *Privacy Act 1988* (Cth) ss 6C, 6D. Businesses with an annual turnover of $3 million or less, however, are bound by the NPPs in certain circumstances such as when the business discloses personal information about another individual for a benefit, service or advantage: see *Privacy Act 1988* (Cth) s 6D(4).

174 Many of these providers were formerly subject to obligations similar to those imposed by the NPPs under the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999). However, this code was repealed when the private sector provisions of the *Privacy Act* commenced in December 2001: see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 56.

175 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [1.2].

63.146 This issue was discussed in the OPC Review and the Senate Committee privacy inquiry. The OPC recommended that the Australian Government consider making regulations under s 6E of the *Privacy Act* to ensure that the Act applied to all small businesses in the telecommunications sector.[176] The Senate Committee recommended that the small business exemption be removed from the *Privacy Act.*[177]

Submissions and consultations

63.147 It was submitted that the development of communications technologies and e-commerce has resulted in more businesses, particularly small to medium businesses, handling large amounts of personal information.[178] A number of stakeholders submitted that, given the high proportion of small business in the telecommunications industry, it was not appropriate to treat small businesses in the telecommunications industry differently from medium and large businesses.[179]

63.148 In its submission to the Inquiry, the OPC reiterated its recommendation in the OPC Review. The OPC noted that there are certain activities that should be regulated because of the nature of the activity, rather than the size of the organisation. This is already the case for the provision of health services, and trading in personal information. The OPC submitted that carriage service providers and ISPs fall into this category because of the amount of personal information they hold, and the potential for adverse impacts on individuals if that information is not protected appropriately.[180]

63.149 Communications Alliance recommended, however, that education and awareness raising and incentives to industry for voluntary adoption of the NPPs would solve the problem. The organisation did not support additional codes which would increase the regulatory burden on small businesses.[181]

ALRC's view

63.150 In Chapter 35, the ALRC proposes the removal of the small business exemption. The implementation of this proposal would solve the problems outlined above. In the meantime, however, the ALRC proposes that the Australian Government make regulations under s 6E of the *Privacy Act* to ensure that the Act applies to all small businesses in the telecommunications industry, including ISPs and public number directory producers.

---

176 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 8.

177 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 12.

178 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

179 Ibid; Law Society of New South Wales, *Submission PR 146,* 29 January 2007; Confidential, *Submission PR 31,* 3 June 2006.

180 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

181 Communications Alliance Ltd, *Submission PR 198,* 16 February 2007.

63.151 The ALRC agrees with the OPC that the risks to privacy posed by small businesses are determined by the amount and nature of personal information held, the nature of the business and the way personal information is handled by the business, rather than by their size alone. The ALRC notes that a number of submissions highlighted that the telecommunications industry, in particular carriage service providers and ISPs, are increasingly handling large amounts of personal information. It is appropriate that the handling of personal information by these organisations is regulated by the *Privacy Act*.

63.152 The ALRC also agrees with Communications Alliance that education has an important role to play in securing compliance with privacy standards. The ALRC acknowledges concerns about the additional compliance burden for small business if they are required to comply with the *Privacy Act*. In Chapter 35, the ALRC discusses ways to reduce the compliance burden on small businesses. The ALRC proposes in Chapter 35 that: a special national helpline for small businesses, similar to the Australian Competition and Consumer Commission's small business helpline, be established; the OPC develop guidelines and other educational material to assist small businesses, and provide free of charge templates for Privacy Policies.

Proposal 63–10 Before the proposed removal of the small business exemption from the *Privacy Act* comes into effect (Proposal 35–1), the Australian Government should make regulations under s 6E of the *Privacy Act* to ensure that the Act applies to all small businesses in the telecommunications industry, including internet service providers and public number directory producers.

Criminal or civil penalties

63.153 A criminal penalty is the only remedy available for a breach of the use and disclosure offences under Part 13 of the *Telecommunications Act*. For example, s 276 provides that a person who contravenes that section is guilty of an offence punishable by imprisonment for a term not exceeding two years. In a regulatory context, criminal sanctions serve as a last-resort punishment after repeated or wilful violations.[182] There have been no prosecutions for breaches of the prohibitions under Part 13 since the *Telecommunications Act* was enacted.

63.154 Should Part 13 of the *Telecommunications Act* attract civil rather than criminal penalties? DCITA submitted that the ALRC might consider whether the administrative and civil regime embodied in the *Privacy Act* is more appropriate than the criminal regime set out in the *Telecommunications Act*.

182 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.40]–[2.44].

63.155 In Chapter 46, the ALRC suggests that there is a need to strengthen the overall enforcement regime of the *Privacy Act*. Accordingly, it proposes that the Act be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual,[183] and for a failure to comply with the proposed data breach notification provisions.[184] Further, in Chapter 55, the ALRC proposes the removal of the credit reporting offences from Part IIIA of the *Privacy Act*, and their replacement with civil penalties where there is a serious or repeated breach of the proposed *Privacy (Credit Reporting Information) Regulations*.[185]

63.156 Civil penalty provisions are founded on the notion of preventing or punishing public harm. The contravention itself may be similar to a criminal offence and may involve the same or similar conduct, and the purpose of imposing a penalty may be to punish the offender, but the procedure by which the offender is sanctioned is based on civil court processes. Civil monetary penalties play a key role in regulation as they may be sufficiently serious to act as a deterrent (if imposed at a high enough level) but do not carry the stigma of a criminal conviction. Civil penalties may be more severe than criminal penalties in many cases.[186] One reason for introducing civil penalties into the *Telecommunications Act* would be to provide punishment for contraventions which fell short of a criminal offence, thus providing ACMA with a greater range of options. The ALRC is interested in stakeholder views on this issue.

Question 63–6 Should a breach of Divisions 2, 4 and 5 of Part 13 of the *Telecommunications Act 1997* (Cth) attract a civil penalty rather than a criminal penalty?

New technologies

63.157 This section considers briefly three relatively new technologies that are considered to have privacy implications—voice over internet protocol (VoIP), electronic numbering (ENUM) and web server logs. These technologies are also discussed in Part B.

Voice over internet protocol

63.158 VoIP enables spoken conversations to be conducted in real time over the internet. VoIP services usually operate over a telecommunications network and are classified as carriage services for the purposes of the *Telecommunications Act*.[187] This

183 Proposal 46–2.
184 Proposal 47–1.
185 Proposal 55–8.
186 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.40]–[2.44].
187 Australian Government Department of Communications Information Technology and the Arts, *Examination of Policy and Regulation Relating to Voice Over Internet Protocol (VOIP) Services* (2005), 19.

means that VoIP service providers will generally be 'carriage service providers' that are required to observe the provisions in Part 13 of the *Telecommunications Act*.

63.159 There are also, however, a variety of VoIP products and services that are closer to pure internet applications in that they tend only to operate over internet protocol networks, and not the Australian Public Switched Telephone Network (PSTN).[188] For example, instant messaging products such as Yahoo Messenger and MSN Messenger allow voice communications from computer to computer over the internet. If a VoIP service does not connect with the PSTN at all, the service provider may not be regulated by the *Telecommunications Act* but may be regulated by the *Privacy Act*.[189] It has been noted that:

> The *Telecommunications Act* does not govern the use of these products and services, and it can be persuasively argued that it does not need to. Those who utilise VoIP products and services of this class have no expectations of a telephony-grade service—they would not, for example, be likely to attempt to make an emergency call using such a service … On the other hand, the privacy issues raised by the use of this class of VoIP products and services are no less real simply because they are not appropriate to be regulated by the *Telecommunications Act*.[190]

63.160 The OPC submitted that it is unclear whether the definition of a 'carriage service provider' in s 87 of the *Telecommunications Act* will always encompass the regulation of ISPs, where ISPs provide services that are similar to those of traditional carriage service providers (for example, where an ISP is hosting VoIP services, which are telephone call services that do not route through the regular PSTN).[191] In the ALRC's view, it is outside the terms of reference for the current Inquiry to consider whether the definition of 'carriage service provider' under s 87 of the *Telecommunications Act* should be amended. This issue should be considered as part of the proposed review of the *Telecommunications Act*.[192]

63.161 Another concern that has arisen in relation to VoIP technology is that Australians may access voice services from providers outside Australia.[193] This may impact on the standards of protection for personal information disclosed during a VoIP call.[194] The OPC Review recommended that the Australian Government initiate discussions in international forums to deal with international jurisdictional issues arising from the global reach of new technologies such as VoIP.[195] The ALRC supports this recommendation.

---

188 The PSTN is the network of the world's public circuit-switched telephone networks. It was originally a network of fixed-line analog telephone systems, but is now almost entirely digital, and includes mobile as well as fixed telephones.

189 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 26.

190 Ibid, 26.

191 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

192 Proposal 63–1.

193 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 25.

194 Ibid, 25.

195 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 70.

ENUM

63.162 ENUM is an abbreviation for electronic numbering or electronic number mapping. ENUM is 'an electronic numbering system that can link the public telephone network and the internet by allowing telephone numbers to be converted into internet domain names'.[196] In summary, ENUM enables telephones connected to the internet to make calls to the PSTN and receive calls from the PSTN.[197] The ALRC notes that ACMA has recently completed a trial of ENUM.[198] It is not known if or when ENUM will become available in Australia.[199]

63.163 ACMA submitted that the next development in ENUM technology, infrastructure ENUM, will involve the mapping of blocks of ENUM registrations 'to a single Internet resource—generally a Voice over Internet Protocol (VoIP) address'.[200] One application of infrastructure ENUM could involve the 'peering'—or direct connection—of VoIP services in isolation from the PSTN.[201]

Web server logs

63.164 Electronic Frontiers Australia noted that it is highly concerned that neither the *Privacy Act* nor the *Telecommunications Act* adequately protect personal information contained in web server logs and similar logs, due in part to an inadequate definition of 'personal information'. It considers that internet protocol addresses should be regarded as 'personal information' because they can be used to identify individuals.

> EFA considers legislative amendments are necessary as a matter of priority to prevent the disclosure of information about Internet users' web browsing activities on the grounds of claims that IP addresses are not personal information and that therefore disclosure and use is not regulated.[202]

63.165 The ALRC considers the definition of 'personal information' in Chapter 3. In that chapter, the ALRC notes that information that simply allows an individual to be contacted—such as an internet protocol address—in isolation, would not fall within the proposed definition of 'personal information'. The *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. Contact information may, however, become 'personal information' in certain contexts, for example, once an internet protocol address is linked to a particular individual.

---

196 Australian Communications Authority, *Annual Report 2004–05* (2005), 36.

197 Australian Communications and Media Authority, *What is ENUM or Electronic Number Mapping?* <www.acma.gov.au> at 30 July 2007.

198 Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 July 2007.

199 ENUM is discussed in more detail in Ch 6.

200 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

201 See, eg, Australian Communications and Media Authority, *Australian ENUM News* (2006) <www.acma.gov.au/WEB/STANDARD//pc=PC_2328> at 30 July 2007.

202 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

ALRC's views

63.166 In Chapter 7, the ALRC suggests that making the *Privacy Act* technologically neutral is the most effective way to ensure individual privacy protection in light of developing technology. Current technologies do not alter fundamentally the nature of the information-handling cycle. The ALRC notes the limitations of the *Telecommunications Act* in dealing with converging technologies in the telecommunications environment. The ALRC proposes that the OPC should provide guidance in relation to technologies that impact on privacy (including, for example, guidance for use of RFID or data collecting software such as 'cookies'). The aim of this guidance is to provide advice on compliance with the proposed UPPs.

63.167 In the ALRC's view, the privacy impact of new communication technologies should be addressed in guidance. ACMA, in consultation with the OPC, Communications Alliance and the TIO, should develop and publish guidance that addresses issues raised by new technologies, such as location-based services, VoIP and ENUM. This guidance should address not only compliance with the proposed UPPs, but also requirements under the *Telecommunications Act* and industry codes and standards.

63.168 In relation to web server logs, the ALRC notes that the use and disclosure offences under Part 13 of the *Telecommunications Act* protect any information or document that relates to the 'affairs or personal particulars (including any unlisted telephone number or any address) of another person'.[203] In the ALRC's view, this information would include an internet protocol address.

Proposal 63–11 The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance and the Telecommunications Industry Ombudsman, should develop and publish guidance that addresses issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.

Telecommunications regulators

63.169 Several bodies are involved in the regulation of the telecommunications industry. ACMA is a statutory authority[204] with specific regulatory powers conferred on it by a number of Acts, including the *Telecommunications Act* and the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth). The TIO is an industry body that investigates and determines complaints by users of

203 See, eg, *Telecommunications Act 1997* (Cth) ss 276, 277.
204 *Australian Communications and Media Authority Act 2005* (Cth) s 8(1).

carriage services,[205] including complaints about privacy.[206] The OPC deals with complaints of interference with privacy in the telecommunications industry. The various issues raised by the involvement of multiple regulators in the telecommunications industry are considered in more detail in Chapter 64. This section of the chapter considers some of the functions of the OPC and ACMA under the *Telecommunications Act*.

Guidance

63.170 The interaction between the *Privacy Act* and the *Telecommunications Act* requires clarification. The ALRC makes a number of proposals aimed at clarifying this interaction. In Chapter 64, the ALRC proposes that the OPC, in consultation with ACMA, Communications Alliance and the TIO, should develop and publish guidance relating to privacy in the telecommunications industry. This guidance should outline the interaction between the *Privacy Act* and the *Telecommunications Act*; provide guidance on the exceptions under Part 13 of the *Telecommunications Act*; and provide guidance about what is required to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

Codes and standards

63.171 Under ss 117 and 134 of the *Telecommunications Act*, the Privacy Commissioner must be consulted about industry codes and standards that deal with privacy issues. In 2005–06, the Privacy Commissioner provided advice in respect of 12 codes being developed pursuant to the *Telecommunications Act*.[207] The Privacy Commissioner must also be consulted:

- before ACMA takes certain steps to promote compliance with an industry code relating to a matter dealt with by the NPPs or an approved privacy code;[208] and
- about the way in which law enforcement bodies certify that disclosure of telecommunications information is reasonably necessary for the enforcement of the criminal law.[209]

63.172 Communications Alliance has developed seven codes under Part 6 of the *Telecommunications Act* which contain privacy provisions or references to relevant privacy legislation.[210] In order to minimise confusion and duplication for the

---

205 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 128(4).
206 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, cl 4.1.
207 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), [1.6.1].
208 *Telecommunications Act 1997* (Cth) ss 121, 122.
209 Ibid s 282(8).
210 Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2003); Australian Communications Industry Forum, *Industry Code—Handling of Life Threatening and Unwelcome Calls Industry Code*, ACIF C525 (2006); Australian Communications Industry Forum,

telecommunications sector, Communications Alliance is in the process of preparing a single industry code which will capture the majority of its consumer industry codes. Communications Alliance is working with the OPC, the TIO, ACMA and the Australian Competition and Consumer Commission to formulate the content of the code. It is also undertaking an extensive public consultation process to enable input by all relevant industry stakeholders.[211]

63.173 The OPC submitted that Part 6 of the *Telecommunications Act* does not define clearly the Privacy Commissioner's powers to comment on whether a code derogates from the *Privacy Act*. In addition, the *Telecommunications Act* does not appear to provide that the Privacy Commissioner must be satisfied with a code before it is registered. The OPC believes that these provisions should be strengthened. For example, s 117 should provide specifically for the Privacy Commissioner to state if, in his or her opinion, the proposed code 'derogates' materially from the provisions of the *Privacy Act*.

63.174 The Australian Privacy Foundation submitted that the use of codes under the *Telecommunications Act* generally has not been successful. Code development takes an enormous amount of time and under resourced consumer groups struggle to make their voices heard in processes designed by and for industry participants. Once approved, adoption is voluntary unless they have been registered by ACMA. Many codes have not been signed by major telecommunications providers. The Australian Privacy Foundation also noted that, even when codes are registered, they are not actively enforced.[212]

ALRC's view

63.175 The ALRC does not propose any major amendments to the code provisions under the *Telecommunications Act*. Part 6 of the *Telecommunications Act* should be considered as part of the proposed review of the *Telecommunications Act*. The ALRC, however, does consider that the provisions relating to the OPC's role in the development of industry codes and standards should be strengthened. The development or amendment of industry codes and standards that deal with matters related to the *Privacy Act* should be subject to a condition that the Privacy Commissioner be consulted, and he or she advise ACMA in writing that he or she is satisfied with the code or standard.

Industry Code—Credit Management, ACIF C541 (2006); Australian Communications Industry Forum, *Industry Code—Billing Industry Code*, C542 (2003); Australian Communications Industry Forum, *Industry Code—Priority Assistance for Life Threatening Medical Conditions Industry Code*, ACIF C609 (2007); Australian Communications Industry Forum, *Integrated Public Number Database (IPND) Data Provider, Data User and IPND Manager*, ACIF C555 (2002); Australian Communications Industry Forum, *Industry Code—Complaint Handling Industry Code*, ACIF C547 (2004).

211 Communications Alliance Ltd, *Submission PR 198,* 16 February 2007.

212 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

Proposal 63–12 Section 117(1)(k) of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority can only register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the code.

Proposal 63–13 Section 134 of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority only can determine, vary or revoke an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, if it has consulted with the Privacy Commissioner, and has been advised in writing by the Privacy Commissioner that he or she is satisfied with the standard.

Reporting

63.176 Part 13 of the *Telecommunications Act* requires carriers, carriage service providers and number database operators to create records of certain disclosures of protected information.[213] These records must be provided to ACMA at the end of each financial year.[214] The Privacy Commissioner monitors compliance with the record-keeping requirements under the Act.[215]

63.177 The OPC noted that it understands that only one reason need be recorded for the disclosure. It suggested that the ALRC consider whether, where there is more than one applicable reason for the disclosure, it would be appropriate for each reason to be recorded.[216] The OPC also noted that participants in the telecommunications industry are not required to report disclosures of information if the disclosure is in the performance of a person's duties; to ASIO; for certain purposes relating to the IPND; by implicit consent of sender and recipient of the communication; or for business needs.[217]

63.178 The OPC also noted that, as part of an enhanced audit and monitoring program over the next few years, the OPC will consider monitoring the record-keeping aspects of relevant disclosures.[218]

213 *Telecommunications Act 1997* (Cth) s 306.
214 Ibid s 308.
215 Ibid s 309.
216 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
217 *Telecommunications Act 1997* (Cth) s 306(1)(b).
218 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

ALRC's view

63.179 It is the ALRC's view that, in the interest of transparency and accountability, when an eligible person or telecommunications provider discloses information or a document pursuant to more than one of the exceptions under Part 13 of the *Telecommunications Act*, each of the exceptions relied upon should be recorded. The recording of these reasons for disclosure will assist ACMA and the OPC to monitor compliance with the Act.

Proposal 63–14 Section 306 of the *Telecommunications Act 1997* (Cth) should be amended to provide that each exception upon which a decision to disclose information or a document is based is to be recorded when that decision is based on more than one of the exceptions in Divisions 3 or 4 of Part 13 of the Act.

A redraft of the Part

63.180 AAPT submitted that it is sometimes difficult to understand the requirements of Part 13 of the *Telecommunications Act*, and that this creates additional confusion in an area already complicated by the proliferation of legislation and regulation.[219]

63.181 The ALRC agrees with the concerns expressed by AAPT and proposes that Part 13 be redrafted to achieve greater logical consistency, simplicity and clarity. As discussed above, the scope of a number of the provisions is unclear—particularly the exceptions to the use and disclosure offences. Part 13 does not follow a logical structure. For example, the exceptions to the use and disclosure offences are separated by the provisions relating to the IPND authorisations. Finally, the provisions relating to the relationship between Part 13 and the *Privacy Act* should be located earlier in the Part.

Proposal 63–15 Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

219 AAPT Ltd, *Submission PR 87,* 15 January 2007.

64. Other Telecommunications Privacy Issues

Contents

Introduction 1901
Interception and access 1901
Telecommunications (Interception and Access) Act 1979 (Cth) 1903
Interaction with the *Privacy Act* 1904
Collection 1905
Use and disclosure 1906
Retention and destruction of records 1909
Reporting requirements 1911
Oversight 1912
The role of the Privacy Commissioner 1915
Spam and telemarketing 1916
Should the *Privacy Act* regulate spam and telemarketing? 1918
Spam Act 2003 (Cth) 1919
Do Not Call Register Act 2006 (Cth) 1926
Telecommunications regulators 1930
Submissions and consultations 1932
ALRC's view 1934

Introduction

64.1 Chapter 63 examined the interaction between the *Privacy Act 1988* (Cth) and the *Telecommunications Act 1997* (Cth). This chapter considers a number of other privacy related telecommunications issues. The first section of the chapter examines access to and interception of information under the *Telecommunications (Interception and Access) Act 1979* (Cth). The next section looks at the regulation of spam and telemarketing under the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).[1] The final section considers options to facilitate cooperation between the various bodies with responsibility for privacy in the telecommunications industry.

Interception and access

64.2 Laws relating to the interception of telecommunications were initially concerned with preserving the integrity of telecommunication systems.[2] In 1960, however, legislation was introduced to protect the privacy of individuals by making it an offence to intercept communications passing over telecommunication systems (with certain

1 Direct marketing is discussed more generally in Ch 23.
2 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [753].

exceptions).[3] In 1979, this Act, and other legislation governing the interception of telecommunications, was repealed and replaced with the *Telecommunications (Interception) Act 1979* (Cth).[4] Since then, there have been a number of inquiries into telecommunications interception and numerous changes to interception legislation.[5]

64.3 Most recently, the *Telecommunications (Interception) Amendment Act 2006* (Cth) amended the *Telecommunications (Interception) Act* to change the name of the Act to the *Telecommunications (Interception and Access) Act 1979* (Cth). The 2006 amendments also implemented a number of the recommendations of the *Report of the Review of the Regulation of Access to Communications* conducted by Mr Anthony Blunn (the Blunn Report).[6]

64.4 The Blunn Report concluded that there was inadequate regulation of access to stored communications, as well as insufficient protection of privacy during the access, storage and disposal processes of stored communications.[7] The *Telecommunications (Interception) Amendment Act* expanded the regulatory telecommunications interceptions scheme by prohibiting access to stored communications, subject to a number of exceptions. It also introduced a regime for the use, disclosure, retention and destruction of accessed stored communications.[8]

64.5 The 2006 amendments broadened the exceptions to prohibited interceptions by introducing 'B-Party' warrants. B-Party warrants are directed to innocent third parties (a 'B-Party') who are likely to communicate with individuals under investigation for serious offences.[9] These controversial amendments are discussed below.

64.6 The Blunn Report concluded that the distribution of provisions between the *Telecommunications Act* and the *Telecommunications (Interception) Act 1979* (as it was then known) dealing with access to telecommunications data for security and law enforcement purposes was 'complicated, confusing and dysfunctional'.[10] The report recommended the introduction of comprehensive legislation dealing with access to all telecommunications and telecommunications data for law enforcement and security

---

3 *Telephonic Communications (Interception) Act 1960* (Cth).

4 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [754]–[755].

5 See, eg, A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department; D Stewart, *Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions* (1986) Australian Government; Parliament of Australia—Joint Select Committee on Telecommunications Interception, *Report* (1986).

6 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department. Mr Blunn is a former Secretary of the Attorney-General's Department.

7 Ibid, [1.8.1].

8 *Telecommunications (Interception and Access) Act 1979* (Cth) ch 3.

9 See, eg, Ibid ss 9(1)(a), 46(1)(d). S Bronitt, J Stellios and K Leong, *Submission PR 213,* 27 February 2007. See also S Bronitt and J Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' (2006) 24 *Prometheus* 414.

10 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, 6.

purposes.[11] The Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) will implement these recommendations.[12]

64.7 The ALRC's current Inquiry is focused on the extent to which the *Privacy Act* and related laws provide an effective framework for the protection of privacy in Australia. As discussed in Chapter 1, in the ALRC's view, communications interception generally is an issue that is outside the scope of this Inquiry. Federal legislation governing the interception of telecommunications, however, contains provisions about the use, disclosure and storage of information which may also be 'personal information'. These provisions, and their interaction with the *Privacy Act,* are within the scope of the Inquiry and are discussed further below.

Telecommunications (Interception and Access) Act 1979 (Cth)

64.8 The *Telecommunications (Interception and Access) Act* makes it an offence to intercept a communication passing over a telecommunications system without the knowledge of the maker of the communication, or to access a 'stored communication'[13] without the knowledge of the sender or intended recipient of the communication.[14] There are exceptions to these general offence provisions. Most importantly, law enforcement agencies can intercept or access communications if they have obtained a warrant to do so. In addition, other individuals, such as employees of telecommunication providers, can intercept or access communications in limited circumstances.[15]

64.9 The *Telecommunications (Interception and Access) Act* provides for two communication interception warrant processes. Part 2.2 of the Act provides for the issuing of warrants authorising the Australian Security and Intelligence Organisation (ASIO) to intercept telecommunications (ASIO warrants). ASIO warrants are issued by the Attorney-General at the request of the Director-General of Security.[16] Part 2.5 sets out a process for the issuing of warrants to agencies other than ASIO to intercept telecommunications. These agencies include Australian Government and state agencies, including a state police force and other bodies such as the Queensland Crime and Misconduct Commission.[17] These warrants (agency warrants) are issued by a judge or a nominated member of the Administrative Appeals Tribunal (AAT).[18]

64.10 The Act also sets out a warrant process for access to stored communications.[19] Whereas the interception warrant regime is limited to law enforcement agencies,

11 Ibid, rec i.
12 The Bill is also discussed in Ch 63.
13 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 6, 7.
14 Ibid s 108.
15 See, eg, Ibid ss 7(2)(a), 108(2)(d).
16 Ibid s 9.
17 Ibid s 34.
18 Ibid s 46.
19 Ibid pt 3.

applications for stored communication warrants can be made by all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This includes the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission.[20] Warrants are issued by an 'issuing authority' appointed by the Attorney-General and may include judges of courts exercising federal jurisdiction, a Federal Magistrate, or a magistrate. The Attorney-General may also appoint AAT members who are legal practitioners of at least 5 years' standing.[21]

64.11 The *Telecommunications (Interception and Access) Act* makes it an offence to record, use or disclose intercepted information, stored communication information, or information about an interception or stored communication warrant, except in certain circumstances.[22] For example, this type of information can be recorded, used or disclosed for the purpose of applying for a warrant or for investigating certain offences.[23]

64.12 The Act also contains a requirement that records of intercepted or stored communications be destroyed in certain circumstances.[24] Law enforcement agencies are obliged to keep records relating to interception and stored communication warrants,[25] and to provide the responsible Minister (currently the Attorney-General)[26] with an annual report containing information about these warrants.[27] The Minister is required to compile information received from law enforcement agencies into a report that must be tabled in Parliament.[28] Civil remedies are also available for unlawful interception of communications.[29]

Interaction with the *Privacy Act*

64.13 It is possible that information intercepted or accessed under the *Telecommunications (Interception and Access) Act* could constitute 'personal information' for the purposes of the *Privacy Act.* Accordingly, the handling of information under the *Telecommunications (Interception and Access) Act* could also be regulated under the *Privacy Act.*

64.14 The acts and practices of ASIO are completely exempt from the requirements of the *Privacy Act*.[30] Consequently, the handling of personal information that has been intercepted or accessed by ASIO will be regulated under the *Telecommunications*

---

20 Ibid s 110; *Telecommunications Act 1997* (Cth) s 282.
21 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6DB.
22 Ibid pt 2.6, pt 3.4 div 2.
23 Ibid ss 63AA, 71, 134, 140.
24 Ibid ss 79 and 150. See discussion below.
25 Ibid pts 2.7, 3.5.
26 Commonwealth of Australia, *Administrative Arrangements Order*, 21 September 2006 [as amended 30 January 2007] sch pt 2.
27 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.8 div 1, pt 3.6 div 1.
28 Ibid pt 2.8 div 2, pt 3.6 div 2.
29 Ibid pts 2.10, 3.7.
30 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2)(a). See Ch 31.

(Interception and Access) Act and privacy guidelines issued by the Attorney General under the *Australian Security and Intelligence Organisation Act 1979* (Cth).[31]

64.15 Most Australian Government law enforcement agencies, such as the Australian Federal Police, are subject to the Information Privacy Principles (IPPs) under the *Privacy Act*.[32] The acts and practices of these agencies in relation to the handling of personal information are therefore regulated by the *Telecommunications (Interception and Access) Act* and the *Privacy Act.*

64.16 The handling of personal information in accordance with the *Telecommunications (Interception and Access) Act* will generally fall within an exception to one of the IPPs, and therefore comply with the *Privacy Act*. For example, the use and disclosure of personal information pursuant to the *Telecommunications (Interception and Access) Act* will be a use or disclosure that is 'required or authorised by or under law' under IPP 10 and IPP 11—and the ALRC's proposed 'Use and Disclosure' Principle.[33] If a law enforcement agency engages in an act or practice that does not comply with the *Telecommunications (Interception and Access) Act*, the act or practice would not be 'authorised by or under law' and so may breach the privacy principles.

Collection

64.17 The interception of, or access to, personal information by a law enforcement agency under the *Telecommunications (Interception and Access) Act* complies with IPP 1 where the collection is 'lawful' and 'necessary for one or more of its functions or activities'. This would also be the case under the proposed 'Collection' Principle.[34]

64.18 The *Telecommunications (Interception) Amendment Act* expanded the circumstances under which stored communications can be accessed to allow 'warrantless' access to stored communications. The *Telecommunications (Interception and Access) Act* allows for stored communications to be accessed without a warrant where one party to that communication has knowledge of the access.[35] A party has 'knowledge' where he or she has been provided with written notice.[36]

64.19 Professor Simon Bronitt, James Stellios and Kevin Leong submitted that this provision creates a regulatory loophole—officials are not required to obtain a warrant to access stored communications in cases where notification is given to one of the parties to a stored communication. It was argued that further consideration must be given to the significance and scope of notification, with careful evaluation of the

31 See discussion in Ch 31.
32 See discussion in Ch 34.
33 See discussion in Ch 22.
34 See Ch 18.
35 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1)(b).
36 Ibid s 108(1A).

reasonable expectations of privacy in relation to stored communications and the competing public interests.[37]

64.20 The ALRC received only one submission on this issue. The ALRC has concerns, however, that this provision allows access to stored communications of many individuals where one participant in a communication has knowledge of the access. For example, a communication involving multiple participants (including non-suspects) such as an online bulletin board could be accessed if one participant in that communication was given written notice of the access. Arguably the collection by an agency of personal information about non-suspect persons is not a collection that is necessary for one or more of its functions or activities. As noted above, however, it is the ALRC's view that the circumstances in which communications can be intercepted is an issue that is outside the scope of this Inquiry. This issue should be considered as part of the review proposed in Chapter 63.[38]

Use and disclosure

64.21 The *Telecommunications (Interception and Access) Act* makes it an offence to record, use or disclose intercepted information, stored communication information, or information about an interception or stored communication warrant, except in certain circumstances.[39] As noted above, the use and disclosure of personal information by agencies pursuant to the *Telecommunications (Interception and Access) Act* is a use or disclosure that is 'required or authorised by or under law' under IPP 10 and IPP 11, and the ALRC's proposed 'Use and Disclosure' Principle.[40]

Dealing in information by organisations

64.22 Sections 63B and 135 of the *Telecommunications (Interception and Access) Act* set out circumstances in which a carrier (which may include a carriage service provider)[41] may communicate or make use of, or communicate to another carrier, lawfully intercepted or accessed information. For example, under ss 63B(1) and 135(3) of the *Telecommunications (Interception and Access) Act*, an employee of a carrier may communicate or make use of lawfully intercepted or accessed information or information that has been obtained by accessing a stored communication in the performance of his or her duties.[42]

64.23 Under ss 63B(2) and 135(4), intercepted and accessed information may be communicated to another carrier if the:

- communication of the information is for the purpose of the carrying on by the other carrier of its business relating to the supply of services by means of a telecommunications network; and

---

37 S Bronitt, J Stellios and K Leong, *Submission PR 213,* 27 February 2007.
38 Proposal 63–1.
39 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.6, pt 3.4 div 2.
40 See Ch 22.
41 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.
42 Ibid ss 63B(1), 135(3).

- information relates to the supply of services by the other carrier by means of a telecommunications network.

64.24 The use and disclosure by telecommunications providers of personal information pursuant to the *Telecommunications (Interception and Access) Act* is a use or disclosure that is 'required or authorised by or under law' under National Privacy Principle 2, and the proposed 'Use and Disclosure' Principle.

64.25 The Australian Communications and Media Authority (ACMA) submitted that 135(4) of the *Telecommunications (Interception and Access) Act* is significantly broader than s 291 of the *Telecommunications Act*, which outlines the circumstances in which information may be disclosed by a carrier or service provider as it relates to their business needs.[43] In ACMA's view, s 135(4) may be used by carriers and carriage service providers to disclose to each other personal information in stored communications that could not have been disclosed under the *Telecommunications Act*.

ALRC's view

64.26 While the ALRC acknowledges that the use and disclosure of intercepted and accessed material may be necessary for the performance of an employee of a carrier's duties, the scope of the exception is unclear. In Chapter 63, the ALRC considers the scope of a similar exception under ss 279 and 296 of the *Telecommunications Act*. The ALRC notes that one option would be to amend ss 279 and 296 to confine the exception to certain specified duties of an employee of a telecommunications provider. Another option would be to limit the exception to uses and disclosures that are related to the primary purpose of collection. The ALRC is interested in views on whether the exception under ss 63B(1) and 150(3) of the *Telecommunications (Interception and Access) Act* requires similar clarification.

64.27 In the ALRC's view, the scope of the exception in relation to the business needs of other carriers under ss 63B(2) and 150(4) of the *Telecommunications (Interception and Access) Act* requires clarification. In Chapter 63, the ALRC considers the scope of a similar exception under s 291 of the *Telecommunications Act*. The ALRC is interested in views on whether and how the exception under ss 63B(2) and 150(4) of the *Telecommunications (Interception and Access) Act* should be clarified.

Question 64–1 Should ss 63B(1) and 135(3) of the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to clarify when an employee of a carrier may communicate or make use of lawfully intercepted or accessed information in the performance of his or her duties?

43 Section 291 of the *Telecommunications Act 1997* (Cth) is discussed in Ch 63.

Question 64–2 How should the provisions that permit an employee of a carrier to communicate to another carrier intercepted or accessed information (ss 63B(2) and 135(4) of the *Telecommunications (Interception and Access) Act*) be clarified?

B-Party warrants

64.28 The Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006 heard a large number of concerns in relation to the interception of B-Party communications.[44] The Committee noted that a principal problem with the B-party warrant is the potential for collecting a great deal of information which may be incidental to, or not even associated with, the investigation for which the warrant was issued.

> As Senator Ludwig noted, 'it is not only the B-party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured'. The result is that potentially not just one, but a great many non-suspects to be caught in the B-party warrant process.[45]

64.29 The Committee recommended that the Bill be amended to introduce defined limits on the use and derivative use of material collected by a B-party warrant.[46] The Australian Government did not accept this recommendation. It noted that material collected by a B-Party warrant is subject to the same rules as other warrants under Part 2.6 of the *Telecommunications (Interception and Access) Act*, and that the derivative use of information is restricted to circumstances where the intercepted information appears to relate to the commission of a serious offence which should be investigated by another agency.[47] Further, the communication of intercepted information by intercepting agencies is subject to the oversight of the Commonwealth Ombudsman and state equivalents.[48]

64.30 The ALRC accepts that the use and disclosure of information obtained by a B-party interception warrant is already governed by the *Telecommunications (Interception and Access) Act.* The ALRC is concerned, however, that there is potential to collect a large amount of information about non-suspect persons under a B-Party warrant compared with other types of warrants. The ALRC did not receive any submissions on this issue, but is interested in views on whether further restrictions should apply in relation to the use and disclosure of information obtained by a B-party interception warrant under the *Telecommunications (Interception and Access) Act.*

---

44 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), ch 4.

45 Ibid, [4.62].

46 Ibid, rec 23.

47 *Telecommunications (Interception and Access) Act 1979* (Cth) s 68.

48 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 11.

Question 64–3 Should further restrictions apply in relation to the use and disclosure of information obtained by a B-party interception warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth)?

Retention and destruction of records

64.31 Section 79 of the *Telecommunications (Interception and Access) Act* provides that a record, 'other than a copy', obtained by means of an interception must be destroyed if the chief officer of an agency is satisfied that it is unlikely that it will be required for certain permitted purposes. The Blunn Report noted that it was curious that the requirement to destroy a record under s 79 did not extend to copies of the record.[49] Section 150 of the Act contains a similar requirement to destroy information or a record obtained by accessing a stored communication. This section, introduced in 2006, does not distinguish between a record and a copy of a record.

64.32 In its submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006, the OPC suggested that s 150 may result in it being 'lawful for an agency to keep irrelevant information indefinitely'. The OPC recommended that

> consideration be given to amending the Bill to ensure that agencies take regular steps to review whether information they have accessed via stored communications warrants is still required for a permitted purpose eg; by setting a maximum period for review.[50]

64.33 The Senate Legal and Constitutional Affairs Committee recommended that the Bill be amended to specify time limits within which an agency must review their holdings of information accessed via a stored communications warrant and destroy information as required under the proposed s 150. The Committee stated its view that, given the potential to collect vast amounts of irrelevant information under a stored communications warrant, such a safeguard was essential.[51]

64.34 In its submission to the current Inquiry, the OPC reiterated its concerns about s 150, noting that it appeared that, until the chief officer has considered the relevant matters, the agency may lawfully keep the information or record. Without greater

---

49 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, [9.4].

50 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006.

51 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [3.79]–[3.80], rec 10.

specificity, the OPC is concerned that in some circumstances it may be lawful for an agency to keep irrelevant information indefinitely.[52]

ALRC's view

64.35 In the ALRC's view, the covert nature of interception and access to communications requires the safeguard that the intercepted or accessed information is destroyed as soon as it is no longer required. The proposed 'Data Security' principle provides that an agency or organisation must take reasonable steps to destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the Unified Privacy Principles (UPPs).[53] In the ALRC's view, this rule should apply to records as well as copies of records of intercepted information. The ALRC proposes that s 79 of the *Telecommunications (Interception and Access) Act* be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

64.36 In the interests of transparency, the Attorney-General's Department should provide guidance on when the chief officer of an agency must cause information or a record to be destroyed when it is no longer needed for a permitted purpose under s 79 and s 150 of the *Telecommunications (Interception and Access) Act*. This guidance should include time limits within which agencies must review holdings of information and destroy information as required by the legislation. In the ALRC's view, this guidance is particularly necessary in relation to stored communications.

Proposal 64–1 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

Proposal 64–2 The Attorney-General's Department should provide guidance on when the chief officer of an agency must cause information or a record to be destroyed when it is no longer required for a permitted purpose under s 79 and s 150 of the *Telecommunications (Interception and Access) Act 1979* (Cth). This guidance should include time limits within which agencies must review holdings of information and destroy information as required by the legislation.

Destruction of non-material content

64.37 The retention and destruction of information obtained by B-Party warrants will be subject to s 79 of the *Telecommunications (Interception and Access) Act*. In its submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the

52 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.
53 See discussion in Ch 25.

Telecommunications (Interception) Amendment Bill 2006, the OPC expressed concern about the absence of rules to require the destruction of material outside the scope of the purpose stated in a B-Party warrant. It recommended 'enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed'.[54] The Committee recommended that there should be strict supervision arrangements introduced to ensure the destruction of non-material content.[55] The Australian Government did not accept this recommendation. It stated that the current rules under the *Telecommunications (Interception and Access) Act* relating to the destruction of information obtained by a warrant under Part 2.6 already require the destruction of this material.[56]

64.38 As noted above, the ALRC is concerned that a large amount of information can be obtained about non-suspects under a B-party warrant, and that copies of records are not currently required to be destroyed under s 79. The ALRC did not receive any submissions in relation to this issue, but agrees with the concerns expressed by the OPC to the Senate Committee. The ALRC therefore proposes that s 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to require expressly the destruction of non-material content intercepted under a B-party warrant.

Proposal 64–3 Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to expressly require the destruction of non-material content intercepted under a B-party warrant.

Reporting requirements

64.39 The *Telecommunications (Interception and Access) Act* sets out various record-keeping and reporting requirements in relation to intercepted telecommunications. For example, ss 80 and 81 of the Act require the chief officer of an agency to keep records of a large number of matters, including particulars of each application for a warrant and details of each warrant issued to the agency.

64.40 Section 100 sets out a large number of reporting requirements about agency warrants, including: the relevant statistics about applications for warrants that an agency made during the year; how many warrants included specified conditions or restrictions relating to the warrant; and the total number of telecommunication services

54 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006.

55 Office of the Privacy Commissioner, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006, rec 24.

56 Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional Legislation Committee Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), 11.

intercepted under particular warrants. Section 102 requires a report to set out information about the effectiveness of warrants, including the number of arrests and convictions recorded on the basis of lawfully intercepted information.

64.41 The record-keeping and reporting requirements in relation to access to stored communications are significantly less onerous than the requirements that apply to the interception of communications.[57] The Australian Privacy Foundation has noted that the large number of occasional users of the stored communications interception regime justifies at least as rigorous, if not greater, accountability mechanisms.[58]

64.42 The Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006 concluded that reporting obligations are vital to provide adequate transparency and accountability for the stored communications warrant regime. The Committee recommended that the Bill be amended to require agencies and the Minister to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants.[59]

64.43 Although the Telecommunications (Interception) Amendment Bill 2006 was amended to provide that reports on access to stored communications must contain information about the effectiveness of warrants, the record-keeping and reporting requirements for stored communications warrants are still less rigorous and detailed than those for other kinds of warrants. The ALRC is interested in whether the *Telecommunications (Interception and Access) Act* should be amended to provide further reporting requirements in relation to the use and effectiveness of stored communications warrants.

Question 64–4 Should the regime relating to access to stored communications under the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to provide further reporting requirements in relation to the use and effectiveness of stored communications warrants?

Oversight

64.44 A number of bodies have oversight of the interception and access of communications under the *Telecommunications (Interception and Access) Act*. As noted above, ASIO warrants are issued by the Attorney-General, and agency warrants are issued by a judge or a member of the AAT. The Inspector General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman both have oversight roles in relation to interception and access of communications. Further, agencies that intercept

57 See *Telecommunications (Interception and Access) Act 1979* (Cth) pt 3.6. See discussion of the ASIO, agency and stored communication warrant regimes above.

58 Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006*, March 2006.

59 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [3.88], rec 11.

and access communications under the Act are also subject to ministerial and parliamentary oversight.[60]

Inspector General of Intelligence and Security

64.45 The IGIS is an independent statutory officer who is responsible for ensuring that Australian intelligence agencies, such as ASIO, conduct their activities legally, behave with propriety, comply with any directions and guidelines from the responsible minister, and have regard for human rights, including privacy.[61] The IGIS therefore has oversight of ASIO in relation to the interception and access of communications under the *Telecommunications (Interception and Access) Act*.

64.46 The IGIS submitted to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception) Amendment Bill 2006 that, because B-Party interception warrants involve a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern, he will give particular attention to this type of warrant.[62]

Commonwealth Ombudsman

64.47 The Commonwealth Ombudsman is an independent statutory office established by the *Ombudsman Act 1976* (Cth). The Act provides that the Ombudsman is to investigate the administrative actions of Australian Government departments and prescribed authorities in response to complaints or on the Ombudsman's own motion. The Commonwealth Ombudsman has oversight of law enforcement bodies, such as the Australian Federal Police, that access and intercept communications under the *Telecommunications (Interception and Access) Act*.[63] Further, the Commonwealth Ombudsman has specific powers under the *Telecommunications (Interception and Access) Act* to enter premises occupied by agencies, obtain relevant material, inspect records and prepare reports in relation to the interception of or access to communications.[64]

Public Interest Monitor

64.48 One issue for consideration is whether the interception of and access to communications under the *Telecommunications (Interception and Access) Act* requires additional oversight. One option, suggested by the Office of the Victorian Privacy Commissioner (OVPC),[65] is the establishment of a Public Interest Monitor (PIM).

---

60 For further discussion of these accountability mechanisms see Ch 31.

61 For a detailed discussion of the Inspector General of Intelligence and Security see Ch 31.

62 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), [4.17].

63 See, eg, *Ombudsman Act 1976* (Cth) ss 5–7.

64 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.7, pt 3.5 div 2.

65 Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007 referring to Office of the Victorian Privacy Commissioner, *Submission to the Australian Government Attorney-General's Department's Review of the Regulation of Access to Communications*, May 2005.

64.49 A PIM was established in Queensland under the *Crime and Misconduct Act 2000* (Qld) and the *Police Powers and Responsibilities Act 1997* (Qld). Under the *Crime and Misconduct Act*, the PIM monitors applications for, and the use of, surveillance warrants and covert search warrants.[66] Under the *Police Powers and Responsibilities Act*, the PIM monitors applications for, and the use of, surveillance device warrants, retrieval warrants and covert search warrants.[67]

64.50 The PIM's primary role is to represent the public interest where law enforcement agencies seek approval to use search powers and surveillance devices which have the capacity to infringe the rights and civil liberties of citizens. The role is based on the public interest in ensuring that law enforcement agencies meet all legislative requirements, and that their proposed actions do not extend beyond the parameters laid down by the Queensland Parliament.

64.51 PIMs perform a variety of functions. For example, under the *Crime and Misconduct Act*, the PIM's functions include:

- appearing at any hearing of an application to a Supreme Court judge or magistrate for a surveillance warrant or covert search warrant to test the appropriateness and validity of the application;
- monitoring the Queensland Crime and Misconduct Commission's compliance with matters concerning applications for surveillance warrants and covert search warrants;
- gathering statistical information about the use and effectiveness of surveillance warrants and covert search warrants; and
- issuing an annual report.[68]

64.52 The ALRC notes that the New South Wales Law Reform Commission (NSWLRC) considered PIMs in its interim report *Surveillance*.[69] In that report, the NSWLRC concluded that the regime recommended in the Report embodied sufficient accountability measures to ensure that public interest concerns are addressed, without the need for a PIM.[70] Accordingly, the NSWLRC did not make a recommendation on this issue, but raised it for further consideration.[71] The ALRC notes that the NSWLRC has since released its final report on surveillance.[72] The final report does not include any consideration of PIMs.

---

66 *Crime and Misconduct Act 2001* (Qld) s 324(1).
67 *Police Powers and Responsibility Act 2000* (Qld) s 740(1).
68 *Crime and Misconduct Act 2001* (Qld) ss 11, 122(1)(b), 149(b), 326–328. See also *Police Powers and Responsibility Act 2000* (Qld) ss 212, 220, 335, 357, 740–745.
69 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001), ch 6.
70 Ibid, [6.47].
71 Ibid, [6.47].
72 New South Wales Law Reform Commission, *Surveillance: Final Report*, Report 108 (2005).

ALRC's view

64.53 The ALRC's preliminary view is that there is adequate oversight of the interception and access of communications under the *Telecommunications (Interception and Access) Act*, but the ALRC is interested in stakeholder views on the need for a PIM. The functions of a PIM at the federal level could include to: appear at an application made by an agency for interception and access warrants; test the validity of a warrant application; gather statistical information about the use and effectiveness of warrants; monitor the retention or destruction of information obtained under a warrant; provide to the IGIS, or other authority as appropriate, a report on non-compliance with the legislation; and report to the Australian Parliament on the use of interception and access warrants.

Question 64–5 Should the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to provide for the role of a public interest monitor? If so, what should be the role of the monitor? Should its role include, for example, to:

(a) appear at any application made by an agency for interception and access warrants under the *Telecommunications (Interception and Access) Act*;

(b) test the validity of warrant applications;

(c) gather statistical information about the use and effectiveness of warrants;

(d) monitor the retention or destruction of information obtained under a warrant;

(e) provide to the Inspector General of Intelligence and Security, or other authority as appropriate, a report on non-compliance with the *Telecommunications (Interception and Access) Act*; or

(f) report to the Australian Parliament on the use of interception and access warrants?

The role of the Privacy Commissioner

64.54 The Australian Mobile Telecommunications Association submitted that the OPC should have a more visible and formally recognised role in the formation of policies affecting telecommunications and law enforcement. This would include the OPC being involved in any reviews of the *Telecommunications (Interception and Access) Act*.[73]

64.55 The Australian Privacy Foundation noted that the Privacy Commissioner has been excluded from the deliberations of the ACMA Law Enforcement Advisory

73 Australian Mobile Telecommunications Association, *Submission PR 154,* 30 January 2007.

Committee. The Foundation submitted that the *Telecommunications Act* expressly should require the Privacy Commissioner to be consulted, preferably through membership of this forum.[74]

64.56 The Law Enforcement Advisory Committee assists ACMA in performing its telecommunications functions as set out in s 8 of the *Australian Communications and Media Authority Act 2005* (Cth), by providing advice and recommendations to ACMA on law enforcement and national security issues relating to telecommunications. The Committee meets on a quarterly basis and is made up of representatives from criminal law enforcement and national security agencies, carriers and carriage service providers, the Australian Government Department of Communications Information Technology and the Arts (DCITA), and the Attorney-General's Department.

64.57 The OPC currently has the capacity to be involved in reviews of the *Telecommunications (Interception and Access) Act.* In the ALRC's view, however, the OPC should have a more formal role in relation to law enforcement issues relating to telecommunications. The OPC should be a member of the ACMA Law Enforcement Advisory Committee. Membership on this Committee would complement its legislative scrutiny function.[75] It also would complement the power proposed in Chapter 44 to allow the Privacy Commissioner to direct an agency or organisation to carry out a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[76]

Proposal 64–4 The Office of the Privacy Commissioner should be made a member of the Australian Communications and Media Authority's Law Enforcement Advisory Committee.

Spam and telemarketing

64.58 'Spam' refers to the use of electronic messaging systems to send unsolicited commercial messages. While the most widely recognised form of spam is email spam, the term is also applied to similar activities in other electronic media, including instant messaging and mobile phone messaging or short message service (SMS) messaging.

64.59 Spam has the potential to threaten the viability and efficiency of electronic messaging by damaging consumer confidence, obstructing legitimate business activity and imposing costs on users.[77] It was recently noted that:

> Spam's growth has been metastatic, both in raw numbers and as a percentage of all mail. In 2001, spam accounted for about five per cent of the traffic on the Internet; by 2004, that figure had risen to more than seventy per cent. This year [2007], in some

74 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
75 *Privacy Act 1988* (Cth) s 27.
76 Proposal 44–4.
77 National Office for the Information Economy, *Spam Act 2003: A Practical Guide for Business* (2004), 2.

> regions, it has edged above ninety per cent—more than a hundred billion unsolicited messages clogging the arterial passages of the world's computer networks every day.[78]

64.60 'Telemarketing' is the marketing of goods and services to the consumer by telephone. Many Australians consider spam and telemarketing to be an invasion of their privacy. In 2005–06, the Telecommunications Industry Ombudsman (TIO) reported that it had received 1,858 complaints about telemarketing.[79] In that same year, ACMA received 2,133 formal complaints, of which 1,796 (84%) related to email spam and 337 (16%) related to SMS spam. ACMA has also reported that it has received 3 million email reports of spam and 1,400 verbal and written enquiries.[80]

64.61 A large number of submissions to the current Inquiry raised concerns about spam and telemarketing.[81] On 1–2 June 2006, the ALRC invited members of the public to contact the ALRC to provide their views and experiences of privacy protection in Australia. This initiative—the National Privacy Phone-In—attracted widespread media coverage, which prompted a large community response. In total, the ALRC received 1,343 responses. The great majority of respondents (73%) nominated telemarketing as their main concern.[82] For example, one member of the public noted:

> I take offence to being phoned at home, particularly after hours, and find these callers very pushy and rude. Due to such callers, we have switched over to a silent home number however we are still receiving calls. This is totally unacceptable. I understand that these people are trying to do their job, but surely there is some way to prevent them from obtaining access to home numbers for the same type of calls over and over again.[83]

64.62 A large number of respondents to the National Privacy Phone-in also considered spam to be an interference with their privacy:

> Today I received an email from an Australian company which I had previously subscribed and then unsubscribed from. The email was along the lines of 'we know you have unsubscribed, if you resubscribe with us you can get a special discount on our products'. I can't believe this is permissible. I unsubscribed, if I wanted to

---

78 M Specter, 'Damn Spam', *The New Yorker* (online), 6 August 2007, <www.newyorker.com>.

79 Telecommunications Industry Ombudsman, *Annual Report 2005–06* (2006), 30, 37.

80 Australian Communications and Media Authority, *ACMA Communications Report 2005–06* (2006), 155.

81 See, eg, A Jackson, *Submission PR 142,* 24 January 2007; L Thomas, *Submission PR 65,* 9 December 2006; G Campbell, *Submission PR 54,* 9 October 2006; N Keele, *Submission PR 53,* 9 October 2006; L Mitchell, *Submission PR 46,* 2 June 2006; P Wikramanayake, *Submission PR 45,* 1 June 2006; J Dowse, *Submission PR 44,* 2 June 2006; L O'Connor, *Submission PR 35,* 2 June 2006; Confidential, *Submission PR 31,* 3 June 2006; M Rickard, *Submission PR 19,* 1 June 2006; Confidential, *Submission PR 13,* 26 May 2006.

82 This was possibly influenced by the fact that a number of media stories about the National Privacy Phone-In focused on telemarketing as a possible concern.

83 *ALRC National Privacy Phone-in*, June 2006, Comment #12.

> resubscribe I would have. This is spam, I consider it to be an intrusion and unacceptable.[84]

Should the *Privacy Act* regulate spam and telemarketing?

64.63 Many small businesses that use spam or engage in telemarketing are exempt from compliance with the *Privacy Act*.[85] Further, the definition of 'personal information' in the *Privacy Act* may not cover information that enables individuals to be contacted, such as email addresses that do not contain a person's name. DCITA gave the following examples:

> Regulating direct marketing activity by regulating the use of 'personal information' therefore has a significant limitation because of the technologies used in direct marketing practices. For example, the making of a telemarketing call using a predictive dialler or the sending of a spam email to an email address that has been randomly generated may not be regulated by the *Privacy Act* as the activities may not necessarily use personal information as defined by the *Privacy Act*.[86]

64.64 In addition, NPP 2 does not apply to, or restrict, the use of personal information for the primary purpose for which it was collected, which could be to engage in telemarketing.[87] NPP 2.1 also explicitly authorises organisations to use personal information for the secondary purpose of direct marketing (which includes telemarketing) in certain circumstances—although an organisation that uses information in this way must offer the individual an option to refuse any further direct marketing communications.

64.65 For these reasons, the *Privacy Act* has left unregulated some practices in the telecommunications context that interfere with privacy. Accordingly, two pieces of federal legislation were introduced to regulate specific activities that impact on privacy in the telecommunications context—the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

Submissions and consultations

64.66 One issue for consideration is whether the *Privacy Act* should regulate spam and telemarketing. One stakeholder submitted that these issues should all be dealt with in the one piece of legislation.[88] The Australian Direct Marketing Association stated, however, that the regulation of specific technology and channels should occur as it does now, through specific legislation such as the *Spam Act* and the *Do Not Call Register Act*.[89]

---

84 *ALRC National Privacy Phone-in*, June 2006, Comment #9.

85 *Privacy Act 1988* (Cth) ss 6C, 6D. The small business exemption is discussed in Ch 35.

86 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

87 The ALRC notes that the proposed 'Direct Marketing' principle will prevent the use and disclosure of personal information for the primary and secondary purpose of direct marketing unless a number of conditions are met. See Ch 22.

88 AAMI, *Submission PR 147,* 29 January 2007.

89 Australian Direct Marketing Association, *Submission PR 298,* 29 June 2007.

64.67 DCITA submitted that the *Spam Act* and the *Do Not Call Register Act* are legislative responses to specific areas of public concern. While these Acts are not intended to derogate from the protection provided in the *Privacy Act*, both pieces of legislation were developed in recognition that regulation of direct marketing activity—such as the sending of commercial electronic messages and the making of telemarketing calls—cannot be achieved effectively solely by protecting the use of personal information.[90]

> Under current legislative arrangements the most effective means of addressing both spam and unwanted telemarketing calls is through communications-specific legislation. This is in recognition that regulation of some direct marketing practices—such as sending of spam email to a randomly generated email address—cannot be achieved by protecting the use of personal information, since personal information is not necessarily what is used to initiate the activity.[91]

ALRC's view

64.68 The ALRC considers that the *Spam Act* and the *Do Not Call Register Act* should continue to regulate spam and telemarketing. In Chapter 23, the ALRC looks at whether the *Privacy Act* should impose a blanket rule for all types and aspects of direct marketing, but suggests that this would be too restrictive. There is a strong view in the community that some forms of direct marketing are more intrusive than others. Those forms of direct marketing should be subject to stronger regulation than applies to less intrusive forms of direct marketing.

64.69 In light of the recent review of the *Spam Act* by DCITA,[92] the introduction of the *Do Not Call Register Act* and the Senate Environment, Communications, Information Technology and the Arts Committee inquiry into that Act,[93] the ALRC does not propose to conduct another detailed study of the *Spam Act* and the *Do Not Call Register Act*. The following section does, however, consider how they interact with the *Privacy Act*.

Spam Act 2003 (Cth)

64.70 The *Spam Act* prohibits the sending of commercial electronic messages via email, SMS, multimedia message service or instant messaging without the consent of the receiver. Accordingly, it establishes an opt-in regime that is different from the provisions governing the use of information for direct marketing in the *Privacy Act*.[94]

---

90 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

91 Ibid.

92 Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).

93 Australian Parliament—Senate Environment, Communications, Information Technology and the Arts Committee, *Inquiry into the provisions of the Do Not Call Register Bill 2006 and the Do Not Call Register (Consequential Amendments) Bill 2006* (2006).

94 *Spam Act 2003* (Cth) s 16. Direct marketing is discussed further in Ch 21.

64.71 The *Privacy Act* provides that 'consent' means 'express consent or implied consent'.[95] Under the *Spam Act*, however, consent can be express and inferred, although it may not be inferred from the mere publication of an electronic address.[96] Consent can be inferred from 'conspicuous publication' of certain electronic addresses, such as the electronic addresses of employees, directors or officers of organisations, so long as the publication is not accompanied by a statement to the effect that the account-holder does not wish to receive unsolicited commercial electronic messages.[97] Regulations may specify in more detail the circumstances in which consent may or may not be inferred.[98] Consent can be withdrawn if the account-holder or a user of the account indicates that he or she does not wish to receive any further commercial electronic messages.[99]

64.72 The *Spam Act* does not prohibit sending 'designated commercial electronic messages'. A commercial electronic message is a 'designated commercial electronic message' if it consists of no more than factual information,[100] or the message is authorised by:

- a government body, registered political party, religious organisation, a charity or charitable institution, and the message relates to goods or services, and the body is the supplier, or prospective supplier, of the goods or services concerned;[101] or
- an educational institution, and the account holder is, or has been, enrolled as a student in that institution or is a member or former member of the household of the relevant electronic account holder and is, or has been, enrolled as a student in that institution, and the message relates to the supply of goods or services, and the educational institution is the supplier, or prospective supplier, of the goods or services concerned.[102]

64.73 The *Spam Act* requires lawful commercial electronic messages to contain certain information, such as information about the identity and contact details of the sender.[103] It also provides that a person must not send a commercial electronic message unless the message includes a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the message, or a statement to similar effect.[104] The requirement to include an unsubscribe message does not apply to designated commercial electronic messages.[105]

---

95 *Privacy Act 1988* (Cth) s 6.
96 *Spam Act 2003* (Cth) sch 2 cl 4. Consent is discussed further in Ch 16.
97 Ibid sch 2 cl 4.
98 Ibid sch 2 cl 5. To date, no such regulations have been made.
99 Ibid sch 2 cl 6.
100 Ibid sch 1 cl 2.
101 Ibid sch 1 cl 3.
102 Ibid sch 1 cl 4.
103 Ibid ss 17.
104 Ibid s 18
105 Ibid s 18(1)(b).

64.74 The *Spam Act* also contains rules prohibiting the supply and use of 'address-harvesting software'[106]—that is, software that is used to search the internet for electronic addresses to compile or 'harvest'.[107] Ordinary telephone calls and facsimile communications are not covered by the Act.[108] ACMA has a range of powers to enable it to enforce the provisions of the *Spam Act*.[109]

64.75 Two industry codes dealing with spam have been developed under the *Telecommunications Act* since the introduction of the *Spam Act*. These are the *Australian eMarketing Code of Practice*[110] and the *Internet Industry Code of Practice*.[111] These codes are intended to complement the operation of the *Spam Act* by outlining action to be taken by industry members to help to counter spam.

64.76 In 2006, the Federal Court of Australia delivered the first significant decision dealing with the *Spam Act*. In *Australian Communications and Media Authority v Clarity1 Pty Ltd*, the Court found that the respondents (Clarity1 and the company's director, Wayne Mansfield) had sent tens of millions of message to recipients whose email addresses had been obtained by the use of harvested address lists.[112] The respondent raised a number of defences which were unsuccessful, including that the recipients of the messages had consented to the sending of the messages because they failed to use the 'unsubscribe facility' in the messages.

64.77 The respondents sought to rely on the OPC-issued *Guidelines to the National Privacy Principles*, which provide in relation to NPP 2 that 'it may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up'.[113] Nicholson J did not accept this argument, finding that non-legislative guidelines do not assist in the interpretation of legislation. Nicholson J also held that the inclusion of an unsubscribe facility in a commercial electronic message does not support an inference that a recipient consented to receiving a message by failing to use the facility. He noted that:

> There are a variety of methods available to recipients to deal with unwanted [commercial electronic messages (CEMs)]. These include simply deleting the CEM without reading it and so being unaware of the unsubscribe facility; ignoring the CEM and/or reporting it to the applicant; utilising a filtering or blocking technique. The sender, in this case Clarity1, would have no way of knowing whether the CEM has

106 Ibid pt 3.
107 Ibid s 4.
108 Ibid s 5(5); *Spam Regulations 2004* (Cth) cl 2.1.
109 *Spam Act 2003* (Cth) pt 4; *Telecommunications Act 1997* (Cth) pt 28. See also Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006), ch 11.
110 Australian eMarketing Code Development Committee, *Australian eMarketing Code of Practice* (2005).
111 Internet Industry Association, *Internet Industry Spam Code of Practice* (2006).
112 *Australian Communications and Media Authority v Clarity1 Pty Ltd* (2006) 150 FCR 494.
113 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 37.

> been opened or read; it is equally open to inference that it may not have been so that the unsubscribe facility was unknown to the recipient.[114]

64.78 In its review of the private sector provisions of the *Privacy Act* (OPC Review), the OPC indicated it would discuss with the Australian Communications Authority (ACA) (now ACMA) the development of guidance to clarify the relationship between the *Privacy Act* and the *Spam Act*.[115] In 2006, DCITA concluded a review of the operation of the *Spam Act*.[116] DCITA found that the Act was operating successfully and should remain unchanged. It recommended, however, that additional advice be developed on the operation of certain aspects of the Act. It also recommended that steps be taken to educate the public about the operation of the Act. To this end it recommended that the OPC and ACMA develop 'joint awareness materials to clarify the relationship between the *Spam Act* and the *Privacy Act*'.[117] DCITA also recommended that the Australian Government undertake further consultation to determine whether facsimile communications should be regulated by the *Spam Act.*

Submissions and consultations

64.79 AAMI noted that the different requirements under the *Spam Act* and the *Privacy Act* contribute to compliance burden and cost, particularly for national businesses that have to develop procedures that comply with both the Acts.[118]

64.80 A number of submissions noted that the *Privacy Act* is inconsistent with the *Spam Act*, because the *Privacy Act* provides an opt-out model for use and disclosure of information for direct marketing, while the *Spam Act* is based on an opt-in model.[119] The Fundraising Institute expressed a preference for an opt-out model.[120] DCITA noted, however, that an opt-out model for the regulation of spam is impracticable:

> Spam is usually sent in an untargeted and indiscriminate manner; includes or promotes offensive or illegal content; is sent in a way that disguises the originator and does not offer a valid and functional address to which respondents may opt-out of receiving further messages. The Department believes that the *Spam Act* provides the best model for the regulation of electronic messaging.[121]

64.81 Electronic Frontiers Australia submitted that, at a minimum, NPP 2 should be amended to be equivalent to the *Spam Act* in relation to consent. It also submitted that

---

114 *Australian Communications and Media Authority v Clarity1 Pty Ltd* (2006) 150 FCR 494, [80].
115 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 11.
116 Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).
117 Ibid, rec 22.
118 AAMI, *Submission PR 147,* 29 January 2007.
119 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007; Australian Direct Marketing Association, *Consultation PC 30*, Sydney, 30 May 2006.
120 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.
121 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.

the *Spam Act* should be amended to require all senders to provide a functional unsubscribe facility and thereby remove the inconsistency with NPP 2.[122]

64.82 The Australian Privacy Foundation submitted that the *Spam Act* and the *Do Not Call Register Act* would not be necessary if there was a properly functioning 'Use and Disclosure' principle in the *Privacy Act*, together with adequate sanctions and active enforcement. The same effect would be achieved if NPP 2 clearly identified unsolicited direct marketing as a secondary use which required express or implied consent.[123]

64.83 ACMA noted that there would be benefits in considering amendments to the *Privacy Act* to reflect the problem of spam. It submitted, however, that the introduction of an opt-in marketing scheme for commercial electronic messages reflects the unique characteristics of email marketing when compared to other forms of direct marketing. ACMA submitted that the *Guidelines on the National Privacy Principles* are now out-of-date in relation to businesses' obligations under the *Spam Act*.[124]

64.84 ACMA also noted that Bluetooth messages may constitute spam but do not meet the definition of 'electronic messages' under s 5 of the *Spam Act* because the messages are sent to electronic addresses (a device's Bluetooth address) in connection with individual devices. The *Spam Act*, however, defines 'electronic message' as being sent to electronic addresses in connection with individual 'accounts'. ACMA submitted that future consideration should be given to whether Bluetooth messages should be regulated by the *Spam Act*.[125]

64.85 The OPC Review recommended that the OPC hold discussions with ACMA on the possibility of issuing joint guidance on the application of the two Acts.[126] The OPC noted, in its submission, that although no joint guidance has been issued to date, it continues to see merit in such an undertaking.[127] DCITA also supported the issuing of guidance on the interaction between the two Acts.[128]

ALRC's view

64.86 As noted above, it is the ALRC's view that the *Spam Act* is an appropriate response to public concern about unsolicited commercial electronic messages.

---

122 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007 referring to Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005.

123 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

124 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007. See also Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.

125 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.

126 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 11, 62–63.

127 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

128 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007. See also Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006), rec 22, 96–7. See also Australian Mobile Telecommunications Association, *Submission PR 154,* 30 January 2007.

However, there is some confusion about the interaction of the *Privacy Act* and the *Spam Act*. The ALRC considers that the OPC, in consultation with ACMA, the Australian Communications Alliance and the TIO, should develop and publish guidance relating to privacy in the telecommunications industry that addresses the interaction between the *Privacy Act* and the *Spam Act*.

64.87 The ALRC acknowledges concerns about the different approaches to opting in under the *Spam Act*, and opting out of direct marketing under the *Privacy Act*. The ALRC agrees with DCITA, however, that the opt-in regime under the *Spam Act* is required to deal with the untargeted and indiscriminate manner in which spam is sent. It is impractical to expect that an individual should have to opt out of the potentially vast number of spam messages sent to a particular address.

64.88 In the ALRC's view, the definitions of 'consent' under the *Privacy Act* and the *Spam Act* are broadly consistent. Further, due to the technology employed to send spam, it is appropriate that the *Spam Act* provides more detailed guidance on when consent can be inferred (for example, from 'conspicuous publication') and that the account holder is the person who can give or withdraw consent. The ALRC considers, however, that the proposed guidance on the interaction between the *Privacy Act* and the *Spam Act* should address what is required to obtain an individual's consent for the purposes of the *Privacy Act* and the *Spam Act*. This guidance should cover consent as it applies in various contexts and include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.[129]

64.89 The ALRC notes that the *Spam Act* does not regulate Bluetooth messages or facsimile messages. Only ACMA addressed this issues in its submission. The ALRC is interested in further views on whether commercial electronic messages sent via these technologies should be regulated by the *Spam Act*.

64.90 The ALRC is also interested in views on whether all commercial electronic messages should be required to include an unsubscribe message, including designated commercial electronic messages sent by organisations such as charities and political organisations and designated commercial electronic messages that consist of no more than factual information. Although it may be appropriate that commercial electronic messages sent by these individuals are exempt from many of the requirements under the *Spam Act*, it is arguable that such messages should include a facility whereby individuals can opt out of receiving further messages.

64.91 In Chapter 23, the ALRC proposes that an organisation must not use or disclose personal information about an individual for the primary purpose or secondary purpose of direct marketing unless a number of conditions are met, including that in each direct marketing communication with an individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications. This would require those bodies that send designated electronic messages to include an unsubscribe message. The ALRC is interested in views on whether the *Spam Act* should also

---

129 See discussion of bundled consent in Ch 16.

provide that designated electronic messages should include an unsubscribe message, or if they should be exempted from that condition under the proposed 'Direct Marketing' principle.

64.92 Further, in Chapter 37, the ALRC suggests that, in the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. The ALRC therefore proposes that registered political parties and political acts and practices should only be exempt under the *Privacy Act* to the extent required to avoid a contravention of the implied freedom of political communication.[130] The Explanatory Memorandum to the *Spam Act* 2003 (Cth) noted that the exception in relation to registered political parties aims to ensure that there is no unintended restriction on religious or political speech.[131] It is arguable, however, that requiring registered political parties to obtain consent before sending commercial electronic messages that relate to goods and services would not necessarily contravene the implied freedom of political communication. The ALRC is interested in hearing further views on this issue.

Question 64–6 Should the *Spam Act 2003* (Cth) be amended to:

(a) provide that the definition of 'electronic message' under s 5 includes Bluetooth messages;

(b) provide that facsimile messages are regulated under the Act;

(c) provide that an electronic message is required to include an unsubscribe message if the electronic message:

  (i) consists of no more than factual information; or

  (ii) has been authorised by a government body, a registered political party, a religious organisation, or a charity or charitable institution, and relates to goods or services; or

  (iii) has been authorised by an educational institution, and relates to goods or services;

(d) remove the exception for registered political parties?

130 Proposal 37–2.

131 Explanatory Memorandum, Spam Bill 2003 (Cth), 107.

Do Not Call Register Act 2006 (Cth)

64.93 The ALRC examined telemarketing (and other forms of direct marketing) in its 1983 report, *Privacy* (ALRC 22).[132] The Report recommended that the Human Rights Commission[133] develop guidelines about telemarketing practices.[134] Since ALRC 22, however, there has been a huge increase in telemarketing activities.[135]

64.94 The OPC Review recommended that the Australian Government consider amending the *Privacy* Act to provide consumers with a right to opt out of receiving all forms of direct marketing at any time,[136] and establishing a 'Do Not Contact' register.[137] The Senate Committee privacy inquiry agreed with the desirability of establishing a 'Do Not Contact' register, but recommended that the ALRC consider, as part of a broader review of the *Privacy* Act, whether an opt-in approach like that adopted by the *Spam Act* should be introduced for all direct marketing.[138]

64.95 On 3 May 2007, the Minister for Communications, Senator Helen Coonan, launched the national Do Not Call Register.[139] The scheme was established under the *Do Not Call Register Act*, which enables the holder of an account for an Australian telephone number to elect not to receive unsolicited telemarketing calls. The Act was introduced in response to 'rising community concerns about the inconvenience and intrusiveness of telemarketing, as well as concerns about the impact of telemarketing on an individual's privacy'.[140]

64.96 The *Do Not Call Register Act* enables account holders, and nominees of account holders, to apply to have their telephone numbers included on a Do Not Call Register held by ACMA. This establishes an opt-out regime that is different from the provisions governing the use of information for direct marketing in the *Privacy Act*.[141] The *Privacy Act* prohibits the use of personal information for the secondary purpose of direct marketing unless an organisation draws an individual's attention to the fact that he or she may opt out of any further direct marketing. The Act also prohibits direct marketing to an individual who has made a request not to receive direct marketing communications. The *Do Not Call Register Act*, however, prohibits the making of unsolicited telemarketing calls without consent to a telephone number on the Do Not Call Register.[142]

---

132 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [88], [252]–[260], [501]–[527], [688]–[691], [1174]–[1182].
133 Now the Human Rights and Equal Opportunity Commission (HREOC).
134 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1182].
135 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth).
136 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), rec 23.
137 Ibid, rec 25.
138 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), rec 15.
139 Australian Communications and Media Authority, 'Do Not Call Register Launched' (Press Release, 3 May 2007).
140 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth).
141 *Do Not Call Register Act 2006* (Cth) ss 13–15. Direct marketing is discussed further in Ch 23.
142 Ibid s 11. Consent is discussed further in Ch 16.

64.97 As noted above, under the *Privacy Act* consent may be express or implied. Under the *Do Not Call Register Act*, consent can be express or inferred, although it cannot be inferred simply from the publication of the telephone number.[143] Regulations may specify in more detail circumstances in which consent may or may not be inferred.[144] If express consent is given, and it is not given for a specified period or for an indefinite period, it is taken to have been withdrawn after three months.[145]

64.98 'Designated telemarketing calls' are exempt from the prohibition on making unsolicited telemarketing calls to a number registered on the Do Not Call Register. 'Designated telemarketing calls' include certain calls authorised by: government bodies; religious organisations; charities or charitable institutions; registered political parties; independent members of the Commonwealth Parliament, a state parliament, or the legislative assembly for an Australian territory, or a local governing body, or a candidate in an election; or educational institutions.[146] In addition, certain telephone numbers—such as numbers used exclusively for the sending or receiving of facsimile communications—cannot be included on the register.[147]

64.99 Telemarketers can request information from ACMA about whether a particular telephone number is on the register.[148] Numbers are registered for a period of three years, after which they are removed from the register unless another valid application for registration of the number is made.[149]

64.100 ACMA has a range of powers to enable it to enforce the provisions of the *Do Not Call Register Act*.[150] In addition, ACMA is required to establish a national industry standard to regulate the conduct of telemarketers, including those exempt from the operation of the Act.[151] On 22 March 2007, ACMA made the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Standard 2007*.[152] The Standard establishes minimum standards in four main areas:

- restricting the calling hours and days for making telemarketing and research calls;
- requiring provision of specific information by the caller;
- providing for the termination of calls; and

143 Ibid sch 2 cl 4.
144 Ibid sch 2 cl 5. To date, no such regulations have been made.
145 Ibid sch 2 cl 3.
146 Ibid sch 2–5.
147 Ibid s 14.
148 Ibid s 20.
149 Ibid s 17.
150 *Do Not Call Register (Consequential Amendments) Act 2006* (Cth) sch 1 pt 2.
151 *Telecommunications Act 1997* (Cth) s 125A.
152 *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Standard 2007*. The standard commenced on 31 May 2007.

- requiring callers to enable calling line identification.[153]

64.101 There is an exception to the rules where consent has been given in advance by the call recipient to receive the call during the prohibited calling hours.[154]

Submissions and consultations

64.102 DCITA considered that the *Do Not Call Register Act* sets out clear obligations for telemarketers, and an easily understandable regime for individuals. DCITA submitted that the *Privacy Act* has not been successful in protecting individuals from unwanted and intrusive telemarketing. It also noted that, in many cases, it is unclear whether information is being collected for the primary or secondary purpose of direct marketing. This makes it difficult for individuals to understand the requirements on the organisation using their personal information.[155]

64.103 DCITA also submitted that the general principles relating to 'consent' under the *Privacy Act* and 'consent' under the *Spam Act* and *Do Not Call Register Act* are broadly consistent. That is, the use and disclosure of certain personal information is limited, but can be used or disclosed with consent, either express or implied. DCITA also noted that the *Do Not Call Register Act* is designed to limit the direct marketing activity received on a telephone number or account. Consequently, the consent arrangements have been specifically designed to reflect those authorised to consent to receiving telemarketing calls on a particular number.

> These consent arrangements are designed to recognise that the account-holder is the most appropriate person to consent to calls made to their telephone number. They are the only individual who can make arrangements in relation to access and use of the telephone.[156]

64.104 The National Australia Bank and MLC noted, however, that the *Privacy Act* and the *Spam Act* do not require consents to include a specified time frame, but the *Do Not Call Register Act* does. They also noted that the different approaches to consent create uncertainty about how an act or practice may be interpreted, both for the organisation and the customer.

> This is because an organisation such as MLC will set out to attain consent from its customer for the use and disclosure of their personal information once and in a single approach. It will not ask a different consent question for each different piece of personal information, therefore this will require taking a common position across the requirements of all legislation that may at times be considered compliant by one regulator but not another.[157]

64.105 The Australian Direct Marketing Association suggested that it is appropriate that the *Do Not Call Register Act* provides for an opt-out regime because it is more

---

153 Ibid ss 5–8.
154 Ibid s 5(5).
155 Australian Government Department of Communications Information Technology and the Arts, *Submission PR 264,* 22 March 2007.
156 Ibid.
157 National Australia Bank and MLC Ltd, *Submission PR 148,* 29 January 2007.

consistent with the *Privacy Act*, and an opt-in regime would decimate the direct marketing industry.[158]

64.106 ACMA submitted that the exemptions for designated telemarketing calls under the *Do Not Call Register Act* allow organisations to make calls to carry out work that is considered to be in the public interest. ACMA noted, however, that exempt organisations must comply with the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Standard 2007*.[159]

64.107 The ALRC heard concerns in consultation meetings and submissions that the exemptions watered down the effect of the Do Not Call Register. For example, one submission noted that, while the development of a Do Not Call Register is welcome, it was disappointing that the Government created an exception for charities, amongst others.[160] Another submission stated:

> I was distressed to see how what I always believed was a right has been emasculated by the exemptions to the Do Not Call Register Bill 2006. The number of organisations that are exempted is far greater than that of those who aren't, effectively making this legislation and the register virtually valueless.[161]

ALRC's view

64.108 The *Do Not Call Register Act* is an appropriate response to the public concerns about telemarketing. The ALRC notes, however, that some stakeholders find the interaction between the *Privacy Act* and the *Do Not Call Register* confusing. The ALRC has suggested that the proposed guidance on privacy in the telecommunications industry should address the interaction between the *Privacy Act* and the *Do Not Call Register Act.*

64.109 Concerns were also expressed in submissions about the different approaches to consent under the *Privacy Act* and the *Do Not Call Register Act*. The definitions of consent under both Acts are broadly consistent. The ALRC notes, however, that the *Do Not Call Register Act* contains additional requirements in relation to consent, including that consent is taken to have been withdrawn at the end of three months. This requirement ensures that telemarketers cannot continue to contact account holders after the time period. Submissions indicate, however, that more guidance is required. The ALRC proposes that the guidance on privacy in the telecommunications industry proposed above address the requirements to obtain an individual's consent for the purposes of the *Privacy Act* and the *Do Not Call Register Act*.

64.110 The ALRC also notes concerns about the authorised exceptions for designated telemarketing calls—especially for politicians and electoral candidates. As noted above, it is the ALRC's view that those who exercise or seek power in

---

158 Australian Direct Marketing Association, *Consultation PC 30*, Sydney, 30 May 2006.
159 Australian Communications and Media Authority, *Submission PR 268,* 26 March 2007.
160 A Johnston, *Submission PR 70,* 31 December 2006.
161 F Pilcher, *Submission PR 17,* 1 June 2006.

government should adhere to the principles and practices that are required of the wider community. The ALRC is therefore interested in hearing views on whether the exception that allows registered political parties, independent members of parliament and candidates in an election to make certain calls to numbers registered on the Do Not Call Register should be removed. The ALRC is conscious of the implied freedom of the political communication and the general public interest in free political discourse. In the ALRC's view, however, it is arguable that the exception could be removed without inhibiting political communication or contravening the constitutional freedom.

64.111 The ALRC also notes that the Explanatory Memorandum to the Do Not Call Register Bill states that the exception would enable political parties to make calls which have a fundraising purpose and would also enable membership drives.[162] In the ALRC's view, however, there are a variety of other methods that political organisations and election candidates can use to raise funds and attract membership that do not involve intrusions into an individual's privacy.

Question 64–7 Should the *Do Not Call Register Act 2006* (Cth) be amended to remove the exception for registered political parties, independent members of parliament and candidates in an election?

Telecommunications regulators

64.112 Several bodies are involved in the regulation of the telecommunications industry. ACMA is a statutory authority[163] with specific regulatory powers conferred on it by a number of Acts, including the *Telecommunications Act*, *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth), *Spam Act* and the *Do Not Call Register Act*.

64.113 The TIO is an external dispute resolution (EDR) scheme that investigates and determines complaints by users of carriage services,[164] including complaints about breaches of the NPPs.[165] The OPC deals with complaints of interference with privacy in the telecommunications industry.

64.114 The Commonwealth Ombudsman inspects, and reports on, actions taken under the *Telecommunications (Interception and Access) Act* by Commonwealth law enforcement agencies.[166] The IGIS also has various oversight powers under the *Telecommunications (Interception and Access) Act*.[167]

64.115 Each of these regulatory bodies receives privacy related complaints from consumers. ACMA noted that concern about privacy was a theme in a number of the

162 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth), 88.
163 *Australian Communications and Media Authority Act 2005* (Cth) s 8(1).
164 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 128(4).
165 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, cl 4.1.
166 Commonwealth Ombudsman, *Submission PR 202,* 21 February 2007.
167 See discussion of the Inspector General of Intelligence and Security above.

complaints it received in 2005–06.[168] In this same period, the TIO received 3,379 complaints relating to privacy of consumers with a landline, mobile telephone or internet connection.[169] In 2005–06, the OPC received 83 complaints about privacy in the telecommunications sector (approximately 7% of all NPP complaints) and 763 telephone enquires about privacy in the telecommunications sector (approximately 4% of all NPP telephone enquiries).[170]

64.116 These regulatory bodies have different powers to resolve complaints. For example, the TIO has the power to order service providers to provide complainants with compensation of up to $10,000.[171] There is no statutory limit on the amount of compensation that the Privacy Commissioner can award to a complainant.[172]

64.117 Submissions to the OPC Review noted that the existence of multiple regulators in the telecommunications industry had the potential to: confuse consumers wishing to complain about telecommunications privacy issues; delay or complicate the resolution of complaints;[173] and waste agency resources.[174] Telstra suggested that industry complaint-handling bodies be given responsibility for considering privacy related complaints at first instance. It submitted that this would ensure the efficient and timely investigation of complaints and enable the OPC to focus on broader privacy issues.[175] The OPC noted that it could work closely with other privacy regulators to

---

168 Australian Communications and Media Authority, *Annual Report 2005–06* (2006), app 7.

169 Telecommunications Industry Ombudsman, *Annual Report 2005–06* (2006), 40, 37, 45. The TIO received almost 600 more privacy complaints in 2005–06 compared to 2004–05 (2,718 complaints): Telecommunications Industry Ombudsman, *Annual Report 2004–05* (2005), 39, 47, 54. Communications Alliance noted that it has conducted an analysis of the privacy related complaints data generated by the TIO as a result of Communications Alliance's review of the Australian Communications Industry Forum, *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, ACIF C523 (1999). This research suggests that the TIO is classifying what are actually telemarketing related complaints as privacy complaints. Further, some of these complaints may be attributed incorrectly to the telemarketing activities of a supplier, when the unsolicited telemarketing activity is the action of an independent telemarketing agency. Communications Alliance submitted that, although the TIO recorded 2,718 complaints relating to privacy in 2004–05, it may be that reported privacy breaches in the telecommunications sector are not as prevalent as the TIO's statistics would suggest: Communications Alliance Ltd, *Submission PR 198,* 16 February 2007.

170 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2005–30 June 2006* (2006), 27, 31.

171 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.1]. It can also recommend the provision of compensation for amounts between $10,000 and $50,000: see *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, [6.2].

172 The powers of the Privacy Commissioner to make determinations are discussed in Ch 45.

173 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [1.3]; Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, 9.

174 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [1.3].

175 Telstra Corporation Limited, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 22 December 2004, [1.7].

'ensure that privacy complaints are handled efficiently and to minimise confusion and costs for both individuals and organisations'.[176]

64.118 Although it is not a regulator, the Australian Communications Alliance plays a key role in the regulation of the telecommunications sector. Membership of the Alliance is drawn from a cross-section of the communications industry, including service providers, vendors, consultants and suppliers as well as business and consumer groups. The Alliance develops and promotes compliance with industry codes. It has put in place a scheme that allows a carrier or carriage service provider to commit formally to comply with Communications Alliance Industry Codes. Part 6 of the *Telecommunications Act* provides that organisations such as Communications Alliance can create industry codes in relation to privacy for the telecommunications sector.

Submissions and consultations

64.119 In IP 31, the ALRC asked whether the existence of overlapping regulators in the telecommunications industry raises any issues. The ALRC asked what bodies (public or private) should be involved in the regulation of personal information in the telecommunications industry.[177]

64.120 Some stakeholders noted that the overlapping complaints regime results in confusion and a loss of confidence by consumers in the ability of the telecommunications industry to handle their complaint;[178] delay in the resolution of complaints;[179] increased compliance costs for telecommunications providers; and duplication of effort by regulators.[180] It was submitted that the regulatory roles of ACMA, the TIO and the OPC, as well as the Communications Alliance should be clarified and relationships strengthened.[181]

64.121 Stakeholders also noted that the existence of multiple complaint handlers can lead to forum shopping. The Australian Mobile Telecommunications Association submitted that this is inefficient and undesirable, for both the individual and the various regulatory and dispute resolution bodies.[182] It was also noted that this places additional pressure on telecommunication suppliers, which may believe that a complaint has been closed but find that it has been re-opened by a separate complaints handling body several months later.[183]

---

176 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.

177 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006), Question 10–3.

178 Telstra, *Submission PR 185,* 9 February 2007; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007; AAPT Ltd, *Submission PR 87,* 15 January 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007; Consumers' Telecommunications Network, *Consultation*, Sydney, 1 February 2007.

179 Telstra, *Submission PR 185,* 9 February 2007; Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.

180 Telstra, *Submission PR 185,* 9 February 2007.

181 Ibid; Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.

182 Australian Mobile Telecommunications Association, *Submission PR 154,* 30 January 2007.

183 AAPT Ltd, *Submission PR 87,* 15 January 2007.

64.122 AAPT submitted that the OPC should be responsible for all telecommunications privacy matters, including complaints handling.[184] Similarly, Telstra submitted that privacy complaints should be dealt with by the OPC in accordance with the framework outlined in the *Privacy Act*.[185]

64.123 Electronic Frontiers Australia submitted, however, that the OPC does not have the resources or the expertise to deal with telecommunications privacy matters. It submitted that it would not support the removal of the telecommunications-specific regulators from the process, because a general complaints body like the OPC is unlikely to be able acquire and maintain sufficient technical knowledge in relation to existing and emerging telecommunications issues.[186]

64.124 AAPT suggested that the OPC is viewed as a 'toothless tiger' because it does not have the legislative power to impose and enforce large penalties.[187] The Fundraising Institute submitted that the OPC has not adequately promoted the *Privacy Act* or provided education and guidance for both agencies and organsiations.[188] The Australian Privacy Foundation submitted that the TIO, as a consumer focused complaint-handling process, has been able to handle some privacy complaints much more quickly and effectively than could the OPC.[189]

64.125 The OPC noted that it may be more efficient for the TIO to handle an individual's complaint which involves both privacy and non-privacy related issues. The OPC submitted, however, that the TIO's jurisdiction to deal with privacy related matters is not equivalent to that of the OPC, whether in terms of the range of matters that can be dealt with, or the type of outcomes that may be available. Further, the OPC noted that the overlap creates the theoretical possibility of each regulator providing divergent views when interpreting the provisions of the *Privacy Act*.[190]

64.126 The OPC submitted that if the TIO retains its role in handling *Privacy Act* complaints in the telecommunications sector, the *Privacy Act* should be amended to provide:

- the Privacy Commissioner with a discretion to decline to investigate, or close a complaint, if an industry ombudsman or similar body has already dealt adequately with the privacy aspects of the complaint, or is currently doing so; and

184 Ibid.
185 Telstra, *Submission PR 185,* 9 February 2007.
186 Electronic Frontiers Australia Inc, *Submission PR 76,* 8 January 2007.
187 AAPT Ltd, *Submission PR 87,* 15 January 2007.
188 Fundraising Institute—Australia Ltd, *Submission PR 138,* 22 January 2007.
189 Australian Privacy Foundation, *Submission PR 167,* 2 February 2007.
190 Office of the Privacy Commissioner, *Submission PR 215,* 28 February 2007.

- for a combined 'decline and referral' power for the Privacy Commissioner, exercisable where an industry ombudsman (or similar body) would be a more appropriate forum to handle the complaint.[191]

ALRC's view

64.127 Stakeholders have suggested that overlapping regulators in the telecommunications industry create a number of problems, including confusion about which body to approach with a privacy complaint and a compliance burden for telecommunications providers. The ALRC has considered various options to deal with the issues raised in submissions, including whether the OPC, or the TIO alone, should deal with telecommunications issues.

64.128 The ALRC considers that there are advantages in having multiple bodies with responsibility for privacy in the telecommunications industry. Industry-specific regulators such as ACMA and TIO, play an important role in this context as they provide industry expertise. Industry-specific regulators also reduce the volume of privacy complaints that would otherwise be made to the OPC, freeing the OPC's resources for other functions. Another potential benefit is peer review and the promotion of high standards of performance.

64.129 In the ALRC's view, however, the relationship between the various bodies with responsibility for telecommunications privacy needs to be strengthened. The ALRC makes a number of proposals aimed at: facilitating cooperation between the OPC, ACMA and the TIO; clarifying the interaction between the legislation that each of the bodies administers;[192] and enhancing public understanding about the privacy obligations of telecommunications providers.

64.130 The ALRC notes that it has only considered the role of each of these bodies in relation to the regulation of privacy. The role and function of each of these bodies in the regulation of the telecommunication industry more broadly should be considered as part of the review proposed in Chapter 63.[193]

New powers of the Privacy Commissioner

64.131 In Chapter 45, the ALRC makes a number of proposals directed to improving the relationship between the OPC and EDR schemes, such as the TIO. The ALRC proposes that the *Privacy Act* be amended to empower the Privacy Commissioner to decline to investigate, or investigate further, a complaint that is already being handled by an EDR scheme.[194]

64.132 The ALRC also proposes that the Privacy Commissioner be empowered both to decline to investigate a complaint and refer it on to an EDR scheme, where the Commissioner is satisfied that the complaint would be handled more suitably by the

---

191 Ibid. See also Office of the Victorian Privacy Commissioner, *Submission PR 217,* 28 February 2007.
192 See discussion of *Telecommunications Act 1997* (Cth) in Ch 63.
193 Proposal 63–1.
194 Proposal 45–2.

scheme.[195] In the ALRC's view, this power should increase transparency around the role of EDR schemes in the privacy context. It should also increase efficiency in dealing with privacy complaints and help provide parties with a 'one-stop-shop' in resolving complaints that are partly about privacy and partly about telecommunications service delivery. The ALRC notes that the EDR schemes under these proposed powers must be approved by the OPC. As noted in Chapter 55, the OPC could be expected to approve EDR schemes with a statutory basis (such as the TIO).

64.133 The ALRC notes further that the OPC currently has the power under the *Privacy Act* not to investigate, or not to investigate further, an act or practice about which a complaint has been made if the Commissioner is satisfied that the act or practice is the subject of an application under another federal law and the subject matter of the complaint has been or is being dealt with adequately under that law, or that law provides a more appropriate remedy.[196] In the ALRC's view, this power would allow the OPC to cease investigating a matter being considered by ACMA under Part 13 of the *Telecommunications Act*.

Memoranda of understanding

64.134 The ALRC notes that the Privacy Commissioner and the New Zealand Privacy Commissioner have entered into an agreement that allows for cooperation on privacy related issues. The Memorandum of Understanding covers the sharing of information related to surveys, research projects, promotional campaigns, education and training programs, techniques in investigating privacy violations and regulatory strategies. Other areas addressed include cooperation on complaints with a cross-border element and the possible undertaking of joint investigations. The Privacy Commissioner has also signed an agreement with the Commonwealth Ombudsman that allows for greater cooperation between their respective offices when dealing with privacy related complaints.

64.135 In the ALRC's view, the OPC, TIO and ACMA should develop memoranda of understanding that address the roles and functions of each of the bodies in relation to complaints handling under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and the *Privacy Act.*

64.136 Such agreements should also address the exchange of relevant information and expertise between the bodies. As the regulator with expertise in privacy, the OPC should provide advice to the TIO in relation to the interpretation of the proposed UPPs, and to ACMA on whether a privacy issue is dealt with better under the *Privacy Act* or the *Telecommunications Act*. Conversely, given that the TIO and ACMA have expertise in telecommunications issues, they should assist the OPC when it is investigating a telecommunications-related privacy matter.

---

195 Proposal 45–2.
196 *Privacy Act 1988* (Cth) s 41.

Proposal 64–5 The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memoranda of understanding, addressing:

(a) the roles and functions of each of the bodies under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Privacy Act*;

(b) the exchange of relevant information and expertise between the bodies; and

(c) when a matter should be referred to, or received from, the bodies.

Complaint-handling policies

64.137 In Chapter 45, the ALRC proposes that the OPC prepare and publish a document setting out its complaint-handling policies and procedures.[197] Consolidating this information into one document should increase the accessibility and transparency of the complaint-handling process, and provide a useful resource for agencies, organisations and individuals. The ALRC also proposes that the OPC should develop and publish enforcement guidelines.[198] Both these documents should set out the roles and functions of the OPC, TIO and ACMA under the *Telecommunications Act*, *Spam Act*, *Do Not Call Register Act* and *Privacy Act*; including when a matter will be referred to, or received from, the TIO and ACMA. The TIO and ACMA also should develop and publish a complaint-handling policy and enforcement guidelines.

Proposal 64–6 The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Proposal 45–8), and its enforcement guidelines (see Proposal 46–2) should address:

(a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and the *Privacy Act*; and

(b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.

197 Proposal 45–8.
198 See Ch 46 and Proposal 46–2.

Guidance

64.138 As noted in Chapter 63, since the deregistration of the Australian Communications Industry Forum *Industry Code—Protection of Personal Information of Customers of Telecommunications Providers*, there is little published guidance on information privacy in the telecommunications industry.

64.139 Submissions to the OPC Review and the current Inquiry indicate that telecommunications providers, regulators and individuals would benefit from the development of such a document, particularly in relation to the interaction between the *Privacy Act* and other legislation that deals with telecommunications privacy issues. The ALRC believes that all bodies with responsibility for telecommunications privacy should be involved in the development of this guidance.

64.140 The guidance should outline the interaction between the *Privacy Act*, *Telecommunications Act*, *Spam Act*, and *Do Not Call Register Act* and include advice on the operation of the exceptions, and on what is required to obtain an individual's consent under each Act. Issues related to exceptions and consent under telecommunications legislation are discussed in more detail above and in Chapter 63.

Proposal 64–7 The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, Australian Communications Alliance and the Telecommunications Industry Ombudsman, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

(a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth);

(b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and

(c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act, Spam Act* and the *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

Educational material

64.141 The ALRC notes that the TIO publishes a number of 'Position Statements' designed to inform the public about a range of telecommunications issues, including privacy. ACMA also publishes on its website some material on Part 13 of the *Telecommunications Act*. There is little information about the operation of the

Telecommunications (Interception and Access) Act on the website of the Australian Government Attorney-General's Department.

64.142 In the ALRC's view, it is important that individuals are aware of agencies and organisations' obligations under telecommunications privacy laws, and know how to seek redress for a breach of those obligations. The ALRC proposes that the OPC, in consultation with ACMA and the TIO, develop and publish educational material that addresses: the rules regulating privacy in the telecommunications industry; the various bodies that are able to deal with a complaint in relation to privacy in the telecommunications industry; and how to make a complaint to those bodies.

64.143 These educational materials should also address agencies and organisations' obligations under the *Telecommunications (Interception and Access) Act*. The OPC should consult with the bodies with responsibility for the administration and oversight of that legislation, namely, the Attorney-General's Department, the IGIS, and the Office of the Commonwealth Ombudsman.

Proposal 64–8 The Office of the Privacy Commissioner, in consultation with the Attorney-General's Department, the Australian Communications and Media Authority, the Office of the Commonwealth Ombudsman, the Inspector General of Intelligence and Security and the Telecommunications Industry Ombudsman, should develop and publish educational material that addresses the:

(a) rules regulating privacy in the telecommunications industry;

(b) various bodies that are able to deal with a complaint in relation to privacy in the telecommunications industry, and how to make a complaint to those bodies.

Appendix 1. List of Submissions

Name	*Submission Number*	*Date*
AAMI	PR 147	29 January 2007
AAPT Ltd	PR 87	15 January 2007
AAPT Ltd	PR 260	20 March 2007
Abacus Australian Mutuals	PR 174	6 February 2007
Abacus Australian Mutuals	PR 278	10 April 2007
ACTU	PR 155	31 January 2007
J Adams	PR 204	21 February 2007
Administrative Appeals Tribunal	PR 201	20 February 2007
Adoption Privacy Protection Group Incorporated	PR 116	15 January 2007
S Alexander	PR 51	18 August 2006
American Express	PR 257	16 March 2007
Anglicare Tasmania	PR 135	19 January 2007
Anonymous	PR 22	20 June 2006
Anonymous	PR 175	6 February 2007
Anonymous	PR 181	6 January 2007
Anonymous	PR 189	10 February 2007
Anonymous	PR 194	8 February 2007
Anonymous	PR 241	9 March 2007

Name	***Submission Number***	***Date***
Anonymous	PR 243	8 March 2007
Anonymous	PR 244	8 March 2007
Anonymous	PR 248	8 March 2007
Anonymous	PR 249	8 March 2007
Anonymous	PR 250	8 March 2007
Anonymous	PR 253	10 February 2007
Anonymous	PR 267	24 March 2007
Anonymous	PR 279	29 March 2007
Anonymous	PR 280	3 April 2007
Anonymous	PR 283	12 April 2007
D Antulov	PR 14	28 May 2006
ANZ	PR 173	6 February 2007
ANZ	PR 291	10 May 2007
Arts Law Centre of Australia	PR 125	15 January 2007
AUSTRAC	PR 216	1 March 2007
Australasian Compliance Institute	PR 102	15 January 2007
Australasian Retail Credit Association	PR 218	7 March 2007
Australia Post	PR 78	10 January 2007
Australian Bankers' Association Inc.	PR 259	19 March 2007
Australian Broadcasting Corporation	PR 94	15 January 2007
Australian Bureau of Statistics	PR 96	15 January 2007
Australian Chamber of Commerce and Industry	PR 219	7 March 2007

Name	***Submission Number***	***Date***
Australian Commission on Safety and Quality in Health Care	PR 252	14 March 2007
Australian Communications and Media Authority	PR 268	26 March 2007
Australian Competition and Consumer Commission	PR 178	31 January 2007
Australian Direct Marketing Association	PR 298	29 June 2007
Australian Electrical and Electronic Manufacturers' Association	PR 124	15 January 2007
Australian Federal Police	PR 186	9 February 2007
Australian Finance Conference	PR 294	18 May 2007
Australian Government Department of Communications, Information Technology and the Arts	PR 264	22 March 2007
Australian Government Department of Employment and Workplace Relations	PR 211	27 February 2007
Australian Government Department of Families, Community Services and Indigenous Affairs	PR 162	31 January 2007
Australian Government Department of Health and Ageing	PR 273	30 March 2007
Australian Government Department of Human Services	PR 136	19 January 2007
Australian Guardianship and Administration Committee	PR 129	17 January 2007
Australian Health Insurance Association	PR 161	31 January 2007

Name	***Submission Number***	***Date***
Australian Institute of Credit Management	PR 224	9 March 2007
Australian Institute of Health and Welfare	PR 170	5 February 2007
Australian Mobile Telecommunications Association	PR 154	30 January 2007
Australian Nursing Federation	PR 205	22 February 2007
Australian Press Council	PR 48	8 August 2006
Australian Press Council	PR 83	12 January 2007
Australian Privacy Foundation	PR 167	2 February 2007
Australian Privacy Foundation	PR 275	2 April 2007
Australian Retailers Association	PR 131	18 January 2007
Australian Security Intelligence Organisation	PR 180	9 February 2007
Australian Taxation Office	PR 168	15 February 2007
AXA	PR 119	15 January 2007
Banking and Financial Services Ombudsman Ltd	PR 263	21 March 2007
M Bartucciotto	PR 62	27 November 2006
P Baum	PR 34	1 June 2006
A Baxter	PR 74	5 January 2007
L Bennett	PR 21	11 June 2006
R Blunden	PR 262	15 March 2007
D Boesel	PR 117	15 January 2007
J Boggs	PR 245	8 March 2007
J Bogotto	PR 140	23 January 2006

Name	***Submission Number***	***Date***
K Bottomley	PR 10	1 May 2006
S Bronitt, J Stellios and K Leong	PR 213	27 February 2007
Business Loans Australia Pty Ltd	PR 282	16 April 2007
L Bygrave	PR 92	15 January 2007
W Caelli	PR 99	15 January 2007
L Callahan	PR 276	2 April 2007
G Campbell	PR 54	9 October 2006
Care Leavers Australia Nework	PR 266	23 March 2007
J Carland and J Pagan	PR 42	11 July 2006
Caroline Chisholm Centre for Health Ethics	PR 69	24 December 2006
Centre for Law and Genetics	PR 127	16 January 2007
Chocolate Messages Pty Ltd	PR 9	1 June 2006
F Churcher	PR 240	9 March 2007
Civil Liberties Australia	PR 98	15 January 2007
P Coad	PR 121	15 January 2007
J Codrington	PR 81	2 January 2007
Commonwealth Ombudsman	PR 202	21 February 2007
Communications Alliance Ltd	PR 198	16 February 2007
Community Services Ministers' Advisory Council	PR 47	28 July 2006
Confidential	PR 5	3 April 2006
Confidential	PR 6	6 March 2006

Name	***Submission Number***	***Date***
Confidential	PR 13	26 May 2006
Confidential	PR 24	6 June 2006
Confidential	PR 27	4 June 2006
Confidential	PR 31	3 June 2006
Confidential	PR 32	2 June 2006
Confidential	PR 49	14 August 2006
Confidential	PR 50	15 August 2006
Confidential	PR 60	27 November 2006
Confidential	PR 88	15 January 2007
Confidential	PR 97	15 January 2007
Confidential	PR 130	17 January 2007
Confidential	PR 132	18 January 2007
Confidential	PR 134	19 January 2007
Confidential	PR 143	24 January 2007
Confidential	PR 165	1 February 2007
Confidential	PR 179	8 February 2007
Confidential	PR 188	9 February 2007
Confidential	PR 206	22 February 200
Confidential	PR 214	27 February 2007
Confidential	PR 223	8 March 2007
Confidential	PR 227	9 March 2007
Confidential	PR 261	17 March 2007

Name	***Submission Number***	***Date***
Confidential	PR 297	1 June 2007
Confidential	PR 312	22 August 2007
J Connor	PR 239	9 March 2007
Consumer Action Law Centre	PR 274	2 April 2007
Consumer Credit Legal Centre (NSW) Inc	PR 28	6 June 2006
Consumer Credit Legal Centre (NSW) Inc	PR 160	31 January 2007
Consumer Credit Legal Centre (NSW) Inc	PR 255	16 March 2007
C Copeland	PR 301	28 June 2007
Council of Small Business Organisations of Australia Ltd	PR 203	21 February 2007
Council of Social Service of New South Wales	PR 115	15 January 2007
CrimTrac	PR 158	31 January 2007
S Crothers	PR 43	14 July 2006
S Crothers	PR 77	8 January 2007
S Crowe	PR 234	2 March 2007
CSIRO	PR 176	6 February 2007
I Cunliffe	PR 37	9 May 2006
T de Koke	PR 8	5 April 2006
Department of Health Western Australia	PR 139	23 January 2006
DLA Phillips Fox	PR 111	15 January 2007
W Dowdell	PR 1	16 February 2006

Name	***Submission Number***	***Date***
J Dowse	PR 44	2 June 2006
J Drake-Brockman	PR 311	17 August 2007
Dun & Bradstreet (Australia) Pty Ltd	PR 11	13 April 2006
Dun & Bradstreet (Australia) Pty Ltd	PR 232	9 March 2007
Edentiti	PR 29	3 June 2006
Edentiti	PR 210	27 February 2007
Electronic Frontiers Australia Inc	PR 76	8 January 2007
Energy and Water Ombudsman NSW	PR 225	9 March 2007
EnergyAustralia	PR 229	9 March 2007
Experian Asia Pacific	PR 228	9 March 2007
Family Law Council	PR 269	28 March 2007
M Fenotti	PR 86	15 January 2007
Finance Sector Union	PR 109	15 January 2007
H Fleming	PR 38	27 June 2006
B Fletcher	PR 296	29 May 2007
Foreign Intelligence Agencies of the Australian Intelligence Community	PR 159	31 January 2007
Free TV Australia	PR 149	29 January 2007
Fundraising Institute–Australia Ltd	PR 138	22 January 2007
K Gardiner	PR 33	1 June 2006
General Electric Capital Finance Australasia Pty Ltd	PR 233	12 March 2007
General Ethical Issues Sub-Committee of the	PR 192	15 February 2007

Name	***Submission Number***	***Date***
Alfred Hospital Ethical Committee		
Justice G Giudice	PR 91	15 January 2007
N Gordon	PR 75	7 January 2007
Government of South Australia	PR 187	12 February 2007
Government of Victoria	PR 288	26 April 2007
G Greenleaf, N Waters and L Bygrave	PR 183	9 February 2007
D Hall	PR 61	27 November 2006
D Hamilton	PR 30	5 June 2006
K Handscombe	PR 52	18 September 2006
K Handscombe	PR 89	15 January 2007
J Harvey	PR 12	25 May 2006
Health and Community Services Complaints Commission (South Australia)	PR 207	23 February 2007
Health Informatics Society of Australia	PR 196	16 January 2007
T Higgins	PR 191	14 February 2007
A Hugo	PR 285	19 April 2007
Human Variome Project	PR 287	23 April 2007
M Hunter	PR 16	1 June 2006
Industry Based Alternative Dispute Resolution Schemes, joint submission	PR 93	15 January 2007
ING Bank	PR 230	9 March 2007
Insolvency and Trustee Service Australia	PR 123	15 January 2007

Name	***Submission Number***	***Date***
Insolvency and Trustee Service Australia	PR 235	12 March 2007
Institute of Mercantile Agents	PR 101	15 January 2007
Institute of Mercantile Agents	PR 270	28 March 2007
Insurance Council of Australia	PR 110	15 January 2007
Investment and Financial Services Association	PR 122	15 January 2007
A Jackson	PR 142	24 January 2007
A Jackson	PR 289	26 April 2007
S Jefferies	PR 295	28 May 2007
A Johnston	PR 70	31 December 2006
A Johnston	PR 251	8 March 2007
N Keele	PR 53	9 October 2006
J Kerr	PR 4	13 March 2006
J Kerr	PR 63	28 November 2006
T Kerr	PR 309	5 August 2007
R Lake	PR 305	19 July 2007
A Lamb	PR 157	31 January 2007
M Lander	PR 58	7 November 2006
M Lander	PR 190	14 February 2007
M Lander	PR 238	9 March 2007
Law Council of Australia	PR 177	8 February 2007
Law Institute of Victoria	PR 200	21 February 2007

Name	***Submission Number***	***Date***
Law Society of New South Wales	PR 146	29 January 2007
P Lee-Archer	PR 20	2 June 2006
Legal Aid Commission of New South Wales	PR 107	15 January 2007
Legal Aid Queensland	PR 212	27 February 2007
Legal Aid Queensland	PR 292	11 May 2007
Link Market Service	PR 2	24 February 2006
L Lucas	PR 95	15 January 2007
A Lyons	PR 290	30 April 2007
M Lyons and B Le Plastrier	PR 41	11 July 2006
R Magnusson	PR 3	9 March 2006
M Maguire	PR 18	1 June 2006
P Maindonald	PR 90	15 January 2007
Mastercard Worldwide	PR 237	13 March 2007
Mental Health Legal Centre Inc	PR 184	1 February 2007
Microsoft Australia	PR 113	15 January 2007
Migration Review Tribunal and Refugee Review Tribunal	PR 126	16 January 2007
Min-it Software	PR 236	13 March 2007
L Mitchell	PR 46	2 June 2006
M Moore	PR 307	3 August 2007
Mortgage and Finance Association of Australia	PR 231	9 March 2007

Name	***Submission Number***	***Date***
National Archives of Australia	PR 199	20 February 2007
National Association for Information Destruction	PR 133	19 January 2007
National Association for the Visual Arts	PR 151	30 January 2007
National Australia Bank and MLC Ltd	PR 148	29 January 2007
National Catholic Education Commission and Independent Schools Council of Australia	PR 85	12 January 2007
National Children's and Youth Law Centre	PR 166	1 February 2007
National Credit Union Association Inc	PR 226	9 March 2007
National E-health Transition Authority	PR 145	29 January 2007
National Health and Medical Research Council	PR 114	15 January 2007
National Legal Aid	PR 265	23 March 2007
National and State Libraries Australasia	PR 68	21 December 2006
S Newton	PR 23	8 June 2006
New South Wales Council for Civil Liberties Inc	PR 156	31 January 2007
New South Wales Guardianship Tribunal	PR 209	23 February 2007
New Zealand Privacy Commissioner	PR 128	17 January 2007
NSW Commission for Children and Young People	PR 120	15 January 2007
NSW Disability Discrimination Legal Centre (Inc)	PR 105	16 January 2007
S Nyman	PR 303	18 July 2007
Obesity Prevention Policy Coalition and	PR 144	25 January 2007

Name	***Submission Number***	***Date***
Young Media Australia		
L O'Connor	PR 35	2 June 2006
C O'Donnell	PR 57	23 October 2006
C O'Donnell	PR 73	5 January 2007
Office of the Health Services Commissioner (Victoria)	PR 153	30 January 2007
Office of the Information Commissioner (Northern Territory)	PR 103	15 January 2007
Office of the NSW Privacy Commissioner	PR 193	15 February 2007
Office of the Privacy Commissioner	PR 215	28 February 2007
Office of the Privacy Commissioner	PR 281	13 April 2007
Office of the Public Advocate Queensland	PR 195	12 February 2007
Office of the Public Advocate Victoria	PR 141	24 January 2007
Office of the Victorian Privacy Commissioner	PR 217	28 February 2007
Q O'Keefe	PR 182	19 January 2007
Optus	PR 258	16 March 2007
P Parker	PR 304	19 July 2007
J Partridge	PR 26	4 June 2006
F Pilcher	PR 17	1 June 2006
Police Federation of Australia	PR 293	14 May 2007
K Pospisek	PR 104	15 January 2007
Public Record Office Victoria	PR 72	3 January 2007

Name	***Submission Number***	***Date***
Queensland Council for Civil Liberties	PR 150	29 January 2007
Queensland Government Commission for Children and Young People and Child Guardian	PR 171	5 February 2007
Queensland Goverment	PR 242	15 March 2007
Queensland Institute of Medical Research	PR 80	11 January 2007
Queensland Law Society	PR 286	20 April 2007
Queensland Police Service	PR 222	9 March 2007
Real Estate Institute of Australia	PR 7	10 April 2006
Real Estate Institute of Australia	PR 84	12 January 2007
W Realph	PR 208	27 February 2007
T Reardon	PR 306	31 July 2007
K Richards	PR 308	2 August 2007
M Rickard	PR 19	1 June 2006
Royal Women's Hospital Melbourne	PR 108	15 January 2007
H Ruglen	PR 39	27 June 2006
Salvation Army	PR 15	2 June 2006
SBS	PR 112	15 January 2007
Social Security Appeals Tribunal	PR 106	15 January 2007
A Smith	PR 79	2 January 2007
K Smith	PR 246	8 March 2007
St George Banking Limited	PR 271	29 March 2007
R Stinson	PR 247	8 March 2007

Name	***Submission Number***	***Date***
T Stutt and L Nicholls	PR 40	11 July 2006
B Such	PR 71	2 January 2007
A Taylor	PR 56	26 October 2006
C Taylor	PR 36	17 June 2006
Telecommunications Industry Ombudsman	PR 221	8 March 2007
Telstra	PR 185	9 February 2007
Tenants Union of NSW Co-op Ltd	PR 169	5 February 2007
Tenants Union of Victoria Ltd	PR 197	16 February 2007
The Mailing House	PR 64	1 December 2006
L Thomas	PR 65	9 December 2006
L Thompson	PR 220	26 February 2007
A Tonking	PR 67	20 December 2006
S Tracey	PR 310	16 August 2007
S Tully	PR 25	7 June 2006
I Turnbull	PR 82	12 January 2007
United Medical Protection	PR 118	15 January 2007
Veda Advantage	PR 163	31 January 2007
Veda Advantage	PR 272	29 March 2007
L Vella	PR 284	17 April 2007
Victorian Automobile Chamber of Commerce	PR 100	15 January 2007
Victorian Society for Computers and the Law Inc	PR 137	22 January 2007

Name	***Submission Number***	***Date***
H Walker	PR 55	20 October 2006
R Ward	PR 254	8 March 2007
N Waters—Cyberspace Law and Policy Centre UNSW	PR 277	3 April 2007
J Watts	PR 302	10 July 2007
Westpac	PR 256	16 March 2007
P Wikramanayake	PR 45	1 June 2006
A Williams	PR 300	28 June 2007
WinMagic Inc	PR 59	24 November 2006
K Wynn	PR 299	20 June 2007
Youth Affairs Council of Victoria Inc	PR 172	5 February 2007
Youthlaw	PR 152	30 January 2007

Appendix 2. List of Agencies, Organisations and Individuals Consulted

Name	*Location*
Abacus–Australian Mutuals	Sydney
Aboriginal Interpreter Service	Darwin
M Abrams, Privacy Consultant	Toronto
Administrative Appeals Tribunal	Sydney
J Alhadeff, Chief Privacy Officer, Oracle	Sydney
ANZ	Melbourne
Professor B Armstrong, Director of Research, Sydney Cancer Centre	Sydney
Australasian Compliance Institute	Sydney
Australasian Epidemiological Association	Melbourne
Australasian Retail Credit Association	Sydney
Australian Broadcasting Corporation	Sydney
Australian Bureau of Statistics	Canberra
Australian Centre for Independent Journalism	Sydney
Australian Chamber of Commerce and Industry	Canberra
Australian Commission on Safety and Quality in Health Care	Sydney
Australian Communications and Media Authority	Sydney
Australian Direct Marketing Association	Sydney
Australian Electoral Commission	Canberra

Australian Federal Police	Canberra
Australian Federation of AIDS Organisations	Sydney
Australian Federation of Travel Agents	Sydney
Australian Finance Conference	Sydney
Australian General Practice Network	Canberra
Australian Government Attorney-General's Department	Canberra
Australian Government Department of Communications, Information Technology and the Arts	Sydney
Australian Government Department of Employment and Workplace Relations	Canberra
Australian Government Department of Families, Community Services and Indigenous Affairs	Canberra
Australian Government Department of Foreign Affairs and Trade	Canberra
Australian Government Department of Health and Ageing	Sydney
Australian Government Department of Human Services	Canberra
Australian Government Department of Prime Minister and Cabinet	Canberra
Australian Government Department of Veterans' Affairs	Canberra
Australian Government Office of Access Card	Canberra
Australian Government Office of Small Business	Canberra
Australian Government Treasury	Canberra
Australian Health Insurance Association	Canberra
Australian Institute of Health and Welfare	Canberra
Australian Institute of Private Detectives	Sydney

Australian Press Council	Sydney
Australian Privacy Foundation	Sydney
Australian Research Alliance for Children and Youth	Perth
Australian Security Intelligence Organisation	Sydney
Australian Subscription Television and Radio Association	Sydney
Australian Taxation Office	Canberra
Banking and Financial Services Ombudsman	Melbourne
A Beatty, Mallesons Stephen Jacques	Sydney
Biometrics Institute	Canberra
Professor J Black, London School of Economics	Sydney
P Black, School of Law, Queensland University of Technology	Brisbane
J King-Christopher, Blake Dawson Waldron	Brisbane
Professor S Bronitt, J Stellios, G Urbas, Faculty of Law, Australian National University	Canberra
T Brookes, Blake Dawson Waldron	Sydney
K Burton, School of Law, Queensland University of Technology	Brisbane
Professor W Caelli, Faculty of Information Technology, Queensland University of Technology	Brisbane
Cancer Australia	Sydney
Cancer Council Victoria	Melbourne
Professor C Cartwright, Aged Services Learning and Research Collaboration, Southern Cross University	Coffs Harbour
Centre for Excellence in Child and Family Welfare	Melbourne

Centre for Law and Genetics	Hobart
Centre for Multicultural Youth Issues	Melbourne
Centrelink	Canberra
CHOICE	Sydney
K Clark, Allens Arthur Robinson	Melbourne
Professor R Clarke, Xamax Consultancy	Canberra
Commonwealth Ombudsman	Canberra
Community Child Care Association	Melbourne
Consumer Credit Legal Centre (NSW)	Sydney
Consumers' Telecommunications Network	Sydney
Credit Corp	Sydney
Professor P Croll, Faculty of Information Technology, Queensland University of Technology	Brisbane
M Crompton and R McKenzie, Information Integrity Solutions	Sydney
P Cullen, Chief Privacy Officer, Microsoft	Sydney
I Cunliffe, Norton White	Melbourne
J Douglas-Stewart, Privacy Law Consulting Australia	Sydney
Dun & Bradstreet	Sydney
K Eastman, Barrister	Sydney
Electronic Frontiers Australia	Brisbane
Embarcadero Technologies	Sydney
Energy and Water Ombudsman New South Wales	Sydney
Fairfax Media Ltd	Sydney

Family Court of Australia	Sydney
Federal Court of Australia	Sydney
Federal Magistrates Court of Australia	Sydney
Professor B Fitzgerald, School of Law, Queensland University of Technology	Brisbane
Free TV Australia	Sydney
GE Commercial	Sydney
GE Money	Sydney
D Giles, Freehills	Sydney
Professor G Greenleaf, Faculty of Law, University of New South Wales	Sydney
Health Consumers Alliance of South Australia	Adelaide
Health Consumers' Council of Western Australia	Perth
High Court of Australia	Sydney
Dr R Hil, School of Arts and Social Sciences, Southern Cross University	Coffs Harbour
G Hill, State Trustees	Melbourne
Hill and Knowlton	Sydney
Dr D Holman, School of Population Health, University of Western Australia	Perth
T Hughes, Executive Director, International Association of Privacy Professionals	Sydney
Office of the Information and Privacy Commissioner, Ontario	Toronto
Inspector-General of Intelligence	Canberra

Institute of Mercantile Agents	Sydney
Insurance Council of Australia	Sydney
Investment and Financial Services Association	Sydney
IMS Health Asia	Sydney
Professor M Jackson, School of Accounting and Law, RMIT University	Melbourne
P Jones, Allens Arthur Robinson	Sydney
Professor B Lane, School of Law, Queensland University of Technology	Brisbane
Law Council of Australia, Privacy Working Group	Sydney
Legal Aid New South Wales	Sydney
Legal Aid Queensland, Consumer Protection Unit	Brisbane
Dr D Lindsay, Faculty of Law, Monash University	Melbourne
D Loukidelis, Information and Privacy Commissioner British Columbia	London
C Lowry, Financial Counsellor	Sydney
A MacRae, former member of the Taskforce on Reducing the Regulatory Burden on Business	Melbourne
Associate Professor R Magnusson, Law School, University of Sydney	Sydney
MasterCard Worldwide	Sydney
Media Entertainment and Arts Alliance	Sydney
Medicare Australia	Canberra
Menzies School of Health Research	Darwin
North Coast Area Health Service	Coffs Harbour

J Moore, Mallesons Stephen Jaques	Sydney
National Aboriginal and Islander Child Care	Melbourne
National Archives of Australia	Canberra
National Children's and Youth Law Centre	Sydney
National E-Health Transition Authority	Canberra
National Health and Medical Research Council Privacy Working Committee	Canberra
New South Wales Commission for Children and Young People	Sydney
New South Wales Council for Civil Liberties	Sydney
New South Wales Law Reform Commission	Sydney
New Zealand Law Commission	Sydney
News Ltd	Sydney
Northern Territory Government Department of Health and Community Services	Darwin
Northern Territory Government Office of the Information Commissioner	Darwin
Office of Northern Territory Solicitor General	Darwin
Office of the New South Wales Privacy Commissioner	Sydney
Office of the Ombudsman Western Australia	Perth
Office of the Privacy Commissioner	Sydney
Office of the Public Advocate Queensland	Brisbane
Office of the Victorian Privacy Commissioner	Melbourne
C Parr, Allens Arthur Robinson	Sydney

Associate Professor M Paterson, Faculty of Law, Monash University	Melbourne
Pharmacy Guild of Australia	Sydney
Dr L Ponemon, Chairman, Ponemon Institute	Sydney
Privacy Committee of South Australia	Adelaide
Public Health Association of Australia	Canberra
Public Interest Advocacy Centre	Sydney
QBE Insurance Group	Sydney
Queensland Government Commission for Children and Young People and Child Guardian	Brisbane
Queensland Government Department of Justice and Attorney-General	Brisbane
Queensland Health	Brisbane
Queensland State Archives	Sydney
Associate Professor M Richardson, Faculty of Law, University of Melbourne University	Melbourne
Sawtell Catholic Care of the Aged	Coffs Harbour
P Schaar, Chairman, Art 29 Data Protection Working Party, and H Neil	London
Sensis Interactive	Sydney
Seven Network Ltd	Sydney
Shopfront Youth Legal Centre	Sydney
A Smith, Mallesons Stephen Jaques	Sydney
South Australian Government Department of the Premier and Cabinet, Social Inclusion Unit	Adelaide

South Australian Government Department for Families and Communities	Adelaide
South Australian Government Department of Health	Adelaide
Professor F Stanley, Executive Director, Australian Research Alliance for Children and Youth	Sydney
State Records Authority of New South Wales	Sydney
State Records of South Australia	Adelaide
State Records Office of Western Australia	Perth
State Solicitor's Office Western Australia	Perth
J Stoddard, Privacy Commissioner Canada	Toronto
Senator N Stott Despoja	Canberra
Suncorp and GIO	Sydney
Assitant Professor D Svantesson, Faculty of Law, Bond University	Brisbane
Dr S Tan, Clinical Advisor, Western Australian Government Department of Health	Perth
Tasmanian Government Department of Health and Human Services	Hobart
Tasmanian Government Office of the Commissioner for Children	Hobart
Tasmanian Ombudsman and Health Complaints Commissioner	Hobart
Telecommunications Industry Ombudsman	Melbourne
Telethon Institute for Child Health Research	Perth
Telstra	Sydney

The Link Youth Health Service	Hobart
R Thomas, Information Commissioner (United Kingdom)	London
P Timmins, Consulting & Training	Sydney
Toyota Finance Australia Ltd	Sydney
Turner Broadcasting System	Sydney
UNISYS Security Index	Sydney
University of New South Wales, Rural Clinical School	Coffs Harbour
Veda Advantage	Sydney
Victorian Government Office of the Health Services Commissioner	Melbourne
N Waters, Pacific Privacy Consulting	Sydney
H Wells, School of Social Sciences, Bond University	Brisbane
Dr N Witzleb, Faculty of Law, University of Western Australia	Perth
Westpac	Sydney
A Waldo, Chief Privacy Officer, Lenovo	Sydney
Western Australian Government Department of Health	Perth
Western Australian Government Office of Children and Youth	Perth
Western Australian Government Office of the Information Commissioner	Perth
Youth Action and Policy Association	Sydney
Youth Affairs Council of Victoria	Melbourne
Youth Substance Abuse Service	Melbourne

Appendix 3. List of Abbreviations

The entities listed below are Australian entities unless otherwise stated.

2000 House of Representatives Committee inquiry	Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000)
2000 Senate Committee inquiry	Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000)
3G	third generation
AAT	Administrative Appeals Tribunal
ABA	Australian Bankers' Association
Abacus	Abacus—Australian Mutuals
ABC	Australian Broadcasting Corporation
ABCI	Australian Bureau of Criminal Intelligence
ABN	Australian Business Number
ABS	Australian Bureau of Statistics
ACA	Australian Communications Authority
ACC	Australian Crime Commission
ACC Act	*Australian Crime Commission Act 2002* (Cth)
ACC Board	Board of the Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Chamber of Industry and Commerce
ACIF	Australian Communications Industry Forum

ACLEI	Australian Commission for Law Enforcement Integrity
ACMA	Australian Communications and Media Authority
ACSI 33	Defence Signals Directorate, *Australian Government Information Technology Security Manual* (ACSI 33) (2004)
ACSI 33	Defence Signals Directorate, *Australian Government Information Technology Security Manual* (ACSI 33) (2004)
ACSQHC	Australian Commission on Safety and Quality in Health Care
ACT	Australian Capital Territory
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
ADMA	Australian Direct Marketing Association
ADR	Alternative Dispute Resolution
Advisory Committee	Privacy Advisory Committee
AEC	Australian Electoral Commission
AFC	Australian Finance Conference
AFP	Australian Federal Police
AFPC	Australian Fair Pay Commission
AGAC	Australian Guardianship and Administration Committee
AGD	Australian Government Attorney-General's Department
AGIMO	Australian Government Information Management Office
AHEC	Australian Health Ethics Committee
AHIA	Australian Health Insurance Association
AHMAC	Australian Health Ministers' Advisory Council
AIC	Australian intelligence community
AIC agencies	Australian intelligence community agencies
AIHW	Australian Institute of Health and Welfare
AIPD	Australian Institute of Private Detectives

AIRC	Australian Industrial Relations Commission
ALGA	Australian Local Government Association
ALRC	Australian Law Reform Commission
ALRC 95	Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002)
ALRC 11	Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979)
ALRC 12	Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979)
ALRC 22	Australian Law Reform Commission, *Privacy*, ALRC 22 (1983)
ALRC 77	Australian Law Reform Commission, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995)
ALRC 85	Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998)
ALRC 96	Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia,* ALRC 96 (2003)
ALRC 98	Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004)
AMA	Australian Medical Association
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*
ANAO	Australian National Audit Office
ANF	Australian Nursing Federation

ANZDATA	Australian and New Zealand Dialysis and Transplant Registry
APC	Australian Press Council
APEC	Asia-Pacific Economic Cooperation
APF	Australian Privacy Foundation
APP Charter	Asia-Pacific Privacy Charter
APPA	Asia Pacific Privacy Authorities Forum
APPC Council	Asia-Pacific Privacy Charter Council
APRA	Australian Prudential Regulation Authority
ARC	Administrative Review Council
ARCA	Australasian Retail Credit Association
ARCA	Australasian Retail Credit Association
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIS	Australian Secret Intelligence Service
Assignees Determination	Privacy Commissioner, *Credit Provider Determination No. 2006–3 (Assignees)* 21 August 2006
ASSPA	Aboriginal Sacred Sites Protection Authority
ATM	Automated Teller Machine
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
AUSTRAC CEO	Chief Executive Officer of AUSTRAC
Austrade	Australian Trade Commission
AVCC	Australian Vice-Chancellors' Committee
Barron and Staten	Professors John Barron and Michael Staten

Beijing Rules	*United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985*
BFSO	Banking and Financial Services Ombudsman
Bio21: MMIM	Bio21: Molecular Medicine Informatics Model
Blunn Report	A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department
CBPRs	cross-border privacy rules
CCeS	Centrelink's Customer Confirmation eService
CCLC	Consumer Credit Legal Centre (NSW)
CCTV	Closed Circuit Television
CDE project	Census Data Enhancement project
CFA	Consumers' Federation of Australia
CIPPIC	Canadian Internet Policy and Public Interest Clinic
Classes of Credit Provider Determination	Privacy Commissioner, *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)* 21 August 2006
CLI	Calling Line Identification
CND	Calling Number Display
COAG	Council of Australian Governments
Code Guidelines	Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001)
Code of Conduct	Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991)
Common Criteria	Common Criteria for Information Technology Security Evaluation
COPPA	*Children's Online Privacy Protection Act 1998* (US)
Council of Europe Convention	Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of*

	Personal Data (1981)
CRAA	Credit Reference Association of Australia
CRN	Customer Reference Number
CROC	United Nations *Convention on the Rights of the Child 1989*
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSMAC	Community Services Ministers' Advisory Council
Data-matching Act	*Data-matching Program (Assistance and Tax) Act 1990* (Cth)
DCITA	Australian Government Department of Communications, Information Technology and the Arts
DEWR	Australian Government Department of Employment and Workplace Relations
DFAT	Australian Government Department of Foreign Affairs and Trade
DIGO	Australian Government Defence Imagery and Geospatial Organisation
DIO	Australian Government Defence Intelligence Organisation
DLU	Data Linkage Unit
DOHA	Australian Government Department of Health and Ageing
DPP	Commonwealth Director of Public Prosecutions
DPS	Department of Parliamentary Services
DRM	Digital Rights Management
DSD	Australian Government Defence Signals Directorate
ECAS	extended credit application summary
EDR	External dispute resolution
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale

ENUM	Electronic Number Mapping
EU	European Union
EU Directive	European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995)
EWON	Energy and Water Ombudsman NSW
Experian	Experian Asia Pacific
FaCSIA	Australian Government Department of Families, Community Services and Indigenous Affairs
FCRA	*Fair Credit Reporting Act 1970* (US)
FDP Act	*Federal Data Protection Act 1990* (Germany).
Flood Report	P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004)
FOI	freedom of information
FOI Act	*Freedom of Information Act 1982* (Cth)
FSU	Financial Services Union
FTC	United States Federal Trade Commission
GBE	government business enterprise
GE Money	GE Capital Finance Australasia
GPS	Global Positioning System
GTMC	Gene Technology Ministerial Council
HIPA Act	*Health Insurance Portability and Accountability Act 1996* (HIPA Act) (US)
HPP	Health Privacy Principle
HREC	Human Research Ethics Committee
HREOC	Human Rights and Equal Opportunity Commission

HTTP	Hypertext Transfer Protocol
ICAO	International Civil Aviation Organisation
ICCPR	*International Covenant on Civil and Political Rights 1966*
IFSA	Investment and Financial Services Association
IGC	Inter-Governmental Committee on the Australian Crime Commission
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986* (Cth)
IHI	Individual Healthcare Identifier
IIA	Internet Industry Association
IMA	Institute of Mercantile Agents
IP	Internet Protocol
IP 31	Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006)
IP 32	Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006)
IPART	NSW Independent Pricing and Regulatory Tribunal
IPND	Integrated Public Number Database
IPND Act	*Telecommunications Amendment (Integrated Public Number Database) Act 2006* (Cth)
IPP	Information Privacy Principle
ISCA	Independent Schools Council of Australia
ISO	International Standards Organisation
ISP	Internet Service Provider
ITSA	Insolvency and Trustee Service Australia
ITU-T	International Telecommunication Union

MAC	mandatory access control
MasterCard	MasterCard Worldwide
MasterCard/ACIL Tasman Report	ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004)
MasterCard/CIE/EDC Report	Centre for International Economics and Edgar Dunn and Company, *Options for Implementation of Comprehensive Credit Reporting in Australia [Prepared for MasterCard Worldwide]* (2006)
MCCA	Ministerial Council on Consumer Affairs
MCEETYA	Ministerial Council on Education, Employment, Training and Youth Affairs
MFAA	Mortgage and Finance Association of Australia
Model Code	*National Standard of Canada Model Code for the Protection of Personal Information* (Canada)
MOU	memorandum of understanding
MRT	Migration Review Tribunal
MRTD	Machine Readable Travel Documents
NAIDWG	National Association for Information Destruction, Australian Members and Stakeholders Working Group
National Archives	National Archives of Australia
National Statement	National Statement on Ethical Conduct in Human Research
NCA	National Crime Authority
NCEC	National Catholic Education Commission
NCRIS	National Collaborative Research Infrastructure Strategy
NCUA	National Credit Union Association
NEAF	National Ethics Application Form
NEHTA	National E-Health Transition Authority

NGN	next generation networks
NHMRC	National Health and Medical Research Council
NHMRC Act	*National Health and Medical Research Council Act 1992* (Cth)
NHPP	National Health Privacy Principle
NIST	National Institute of Standards and Technology
NPII	National Personal Insolvency Index
NPP	National Privacy Principle
NSWLRC	New South Wales Law Reform Commission
NSWLRC CP 1	New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007)
NZ Code	*Credit Reporting Privacy Code 2004* (NZ)
NZLC	New Zealand Law Commission
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)
OECD Security Guidelines	Organisation for Economic Co-operation and Development *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002)
ONA	Australian Government Office of National Assessments
OPC	Office of the Privacy Commissioner
OPC Review	Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act 1988* (Cth)
OPPC	Obesity Prevention Policy Coalition
OVPC	Office of the Victorian Privacy Commissioner
P3P	Platform for Privacy Preferences
PC	personal computer

PCI	Payment Card Industry
PDA	personal digital assistant
PETs	privacy enhancing technologies
PIA	Privacy Impact Assessment
PIA Guide	Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006)
PID	Public Interest Determination
PIM	Public Interest Monitor
PIPED Act	*Personal Information Protection and Electronic Documents Act 2000* (Canada)
PIPP	Personal Information Protection Principle
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PPS	Payment Performance System
PRIME	Privacy Identity Management for Europe
Privacy Act	*Privacy Act 1988* (Cth)
Privacy NSW	Office of the NSW Privacy Commissioner
PSIS	Prescription Shopping Information Service
PSM 2005	Australian Government Attorney-General's Department, *Protective Security Manual* (2005)
PSTN	Public Switched Telephone Network
Regulatory Taskforce	Taskforce on Reducing Regulatory Burdens on Business
REIA	Real Estate Institute of Australia
RFID	Radio Frequency Identification
RIS	Regulatory Impact Statement
RRT	Refugee Review Tribunal

RTD	Residential Tenancy Database
SALRC	South African Law Reform Commission
SBS	Special Broadcasting Service
SCAG	Standing Committee of Attorneys-General
SCNS	Secretaries Committee on National Security
SCOR	Steering Committee on Reciprocity
Section 95 Guidelines	Guidelines under s 95 of the *Privacy Act 1988* (Cth)
Section 95A Guidelines	Guidelines Approved under s 95A of the *Privacy Act 1988* (Cth)
SEHR	Shared Electronic Health Record
Senate Committee privacy inquiry	Parliament of Australia—Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth)
SIM	Subscriber Identity Module
SLCD	Statistical Longitudinal Census Dataset
SSAT	Social Security Appeals Tribunal
State Records	State Records of South Australia
TFN	Tax File Number
TIO	Telecommunications Industry Ombudsman
TPA	*Trade Practices Act 1974* (Cth)
TPID	Temporary Public Interest Determination
UHI	Unique Healthcare Identifier
UN	United Nations
UPP	Unified Privacy Principle
URL	Uniform Resource Locater
US Interagency Guidance	United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation,

	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (2005).
US Patriot Act	*Uniting and Strengthening America by Providing Appropriate Tools to Interact and Obstruct Terrorism Act 2001* (US)
VACC	Victorian Automobile Chamber of Commerce
Victorian Review	2006 Victorian Consumer Credit Review
VLRC	Victorian Law Reform Commission
VoIP	Voice over Internet Protocol
VSCL	Victorian Society for Computers and the Law
W3C	World Wide Web Consortium
Wallis report	Financial System Inquiry Committee, *Financial System Inquiry Final Report* (1997)
Web	World Wide Web
YACVic	Youth Affairs Council of Victoria
YMA	Young Media Australia

Reports of the Australian Law Reform Commission

(Not including Annual Reports)

ALRC 1 Complaints Against Police, 1975
ALRC 2 Criminal Investigation, 1975
ALRC 4 Alcohol, Drugs and Driving, 1976
ALRC 6 Insolvency: The Regular Payment of Debts, 1977
ALRC 7 Human Tissue Transplants, 1977
ALRC 9 Complaints Against Police (Supplementary Report), 1978
ALRC 11 Unfair Publication: Defamation and Privacy, 1979
ALRC 12 Privacy and the Census, 1979
ALRC 14 Lands Acquisition and Compensation, 1980
ALRC 15 Sentencing of Federal Offenders (Interim), 1980
ALRC 16 Insurance Agents and Brokers, 1980
ALRC 18 Child Welfare, 1981
ALRC 20 Insurance Contracts, 1982
ALRC 22 Privacy, 1983
ALRC 24 Foreign State Immunity, 1984
ALRC 26 Evidence (Interim), 1985
ALRC 27 Standing in Public Interest Litigation, 1985
ALRC 28 Community Law Reform for the Australian Capital Territory: First Report: The Community Law Reform Program. Contributory Negligence in Fatal Accident Cases and Breach of Statutory Duty Cases and Funeral Costs in Fatal Accident Cases, 1985
ALRC 30 Domestic Violence, 1986
ALRC 31 The Recognition of Aboriginal Customary Laws, 1986
ALRC 32 Community Law Reform for the Australian Capital Territory: Second Report: Loss of Consortium and Compensation for Loss of Capacity to do Housework, 1986
ALRC 33 Civil Admiralty Jurisdiction, 1986
ALRC 35 Contempt, 1987
ALRC 36 Debt Recovery and Insolvency, 1987
ALRC 37 Spent Convictions, 1987
ALRC 38 Evidence, 1987
ALRC 39 Matrimonial Property, 1987
ALRC 40 Service and Execution of Process, 1987
ALRC 42 Occupiers' Liability, 1988
ALRC 43 The Commonwealth Prisoners Act, (Interim) 1988
ALRC 44 Sentencing, 1988
ALRC 45 General Insolvency Inquiry, 1988
ALRC 46 Grouped Proceedings in the Federal Court, 1988
ALRC 47 Community Law Reform for the Australian Capital Territory: Third Report: Enduring Powers of Attorney, 1988
ALRC 48 Criminal Admiralty Jurisdiction and Prize, 1990
ALRC 50 Informed Decisions About Medical Procedures, 1989
ALRC 51 Product Liability, 1989
ALRC 52 Guardianship and Management of Property, 1989
ALRC 55 Censorship Procedure, 1991
ALRC 57 Multiculturalism and the Law, 1992
ALRC 58 Choice of Law, 1992
ALRC 59 Collective Investments: Superannuation, 1992
ALRC 60 Customs and Excise, 1992
ALRC 61 Administrative Penalties in Customs and Excise, 1992
ALRC 63 Children's Evidence: Closed Circuit TV, 1992
ALRC 64 Personal Property Securities, 1993
ALRC 65 Collective Investments: Other People's Money, 1993
ALRC 67 Equality Before the Law: Women's Access to the Legal System, (Interim) 1994
ALRC 68 Compliance with the *Trade Practices Act 1974*, 1994
ALRC 69 Equality Before the Law: Justice for Women, 1994
ALRC 70 Child Care for Kids: Review of Legislation Administered By Department of Human Services and Health, (Interim) 1994
ALRC 72 The Coming of Age: New Aged Care Legislation for the Commonwealth, 1995
ALRC 73 For the Sake of the Kids: Complex Contact Cases and the Family Court, 1995
ALRC 74 Designs, 1995
ALRC 75 Costs Shifting: Who Pays for Litigation, 1995
ALRC 77 Open Government: A Review of the Federal *Freedom of Information Act 1982*, 1995
ALRC 78 Beyond the Door-Keeper: Standing to Sue for Public Remedies, 1996
ALRC 79 Making Rights Count: Services for People With a Disability, 1996
ALRC 80 Legal Risk in International Transactions, 1996
ALRC 82 Integrity: But Not By Trust Alone: AFP & NCA Complaints and Disciplinary Systems, 1996
ALRC 84 Seen and Heard: Priority for Children in the Legal Process, 1997
ALRC 85 Australia's Federal Record: A Review of *Archives Act 1983*, 1998
ALRC 87 Confiscation That Counts: A Review of the *Proceeds of Crime Act 1987*, 1999
ALRC 89 Managing Justice: A Review of the Federal Civil Justice System, 2000
ALRC 91 Review of the *Marine Insurance Act 1909*, 2001
ALRC 92 The Judicial Power of the Commonwealth: A Review of the *Judiciary Act 1903* and Related Legislation, 2001
ALRC 95 Principled Regulation: Federal Civil & Administrative Penalties in Australia, 2002
ALRC 96 Essentially Yours: The Protection of Human Genetic Information in Australia, 2003
ALRC 98 Keeping Secrets: The Protection of Classified and Security Sensitive Information, 2004
ALRC 99 Genes and Ingenuity: Gene Patenting and Human Health, 2004
ALRC 102 Uniform Evidence Law, 2005
ALRC 103 Same Crime, Same Time: Sentencing of Federal Offenders, 2006
ALRC 104 Fighting Words: A Review of Sedition Laws in Australia, 2006